UNIVERZITET SINGIDUNUM



Gojko Grubor
Milan Milosavljević

OSNOVE ZAŠTITE INFORMACIJA

Metodološko - tehnološke osnove

BEOGRAD, 2010.

UNIVERZITET SINGIDUNUM

Gojko Grubor
Milan Milosavljević

OSNOVE ZAŠTITE INFORMACIJA

Metodološko - tehnološke osnove

Beograd, 2010.

OSNOVE ZAŠTITE INFORMACIJA: Metodološko - tehnološke osnove

Autori:
Doc. dr Gojko Grubor
Prof. dr Milan Milosavljević

Recenzenti:
Prof. dr Milovan Stanišić
Prof. dr Branko Kovačević

Izdavač:
UNIVERZITET SINGIDUNUM
Beograd, Danijelova 32
www.singidunum.ac.rs

Za izdavača:
Prof. dr Milovan Stanišić

Tehnički urednik:
Novak njeguš

Dizajn korica:
Aleksandar Mihajlović

Lektor:
Snježana Krstić

Godina izdanja:
2010.

Tiraž:
300 primeraka

Štampa:
Mladost Grup
Loznica

ISBN 978-87-7912-313-8

Copyright:
© 2010 Univerzitet Singidunum
Izdavač zadržava sva prava.
Reprodukcija pojedinih delova ili celine ove publikacije nije dozvoljena.



PREDGOVOR

Udžbenik **Osnove zaštite informacija** – *metodološko tehnološke osnove* je drugo izdanje, prošireno, obnovljeno i ažurirano sa savremenim trendovima u oblasti zaštite informacija u elektronskom okruženju. Namenjen je studentima osnovnih studija i u osnovi je usklađen sa silabusom predmeta *Osnove zaštite informacija*. Udžbenik sadrži i šire informacije iz oblasti zaštite informacija u elektronskom okruženju, tako da ga mogu koristiti i profesionalci u zaštiti, koji žele sistematizovati i upotpuniti svoja znanja.

Glavni cilj pisanja ovog udžbenika je, da se raznovrsna i obimna teorija, dostupna uglavnom u stranoj literaturi, standardima i autorskim radovima na Internetu, sistematizuje, terminološki ujednači i približi studentima i prosečnim korisnicima IKT sistema, koji žele unaprediti znanja u kompleksnoj oblasti zaštite informacija. Smanjenje kompleksnosti terminologije zaštite jedan je od strateških ciljeva teorije i prakse zaštite. Time se postiže veća razumljivost i bolja korisnička prihvatljivost zaštite informacija, što je često problem za obične korisnike, menadžere i vlasnike IKT sistema. Brojni funkcionalni, grafički, strukturni i objektno orijentisani modeli, uzorci i primeri dati u udžbeniku i prilozima, koji je sastavni deo udžbenika, takođe, doprinose smanjenju kompleksnosti problematike zaštite informacija u elektronskom okruženju.

Metodološki, udžbenik je koncipiran u dve glave: *Bezbednost informacionih sistema* i *Upravljanje sistemom zaštite informacija*. Svako poglavlje je struktuirano modularno, sa uvodom, razradom razmatranog problema, rezimeom, ključnim terminima i pitanjima za ponavljanje. Spisak korišćene i šire literature dat je na kraju svake glave.

Za obradu celokupne problematike zaštite informacija u elektronskom okruženju korišćeni su i razmatrani koncepti: *terminologije zaštite, strateškog* i *taktičkog* rešavanja problema zaštite, *reaktivnih* i *proaktivnih sistema zaštite*, *sistemskog, procesnog i objektno orijentisanog pristupa* zaštiti informacija.

U prvoj glavi definisani su i opisani u 9 poglavlja metodološke i tehnološke osnove zaštite poslovnih IKT sistema, odnosno, informacija kao najvrednije imovine svake organizacije. Metodološki aspekt obuhvata: definicije ključnih termina; principe, relevantne standarde i normative zaštite; koncepte *reaktivne* i *proaktivne* zaštite; koncepte servisa, mehanizama i *kontrola zaštite*; metodologije i modele zaštite. Tehnološki aspekt obuhvata osnovne tehnike i alate zaštite računarskih sistema i računarskih mreža.

U drugoj glavi**,** *Upravljanje sistemom zaštite informacija,* u 9 poglavlja obrađene su: upravljačke, operativne i kontrolne komponente zaštite, uključujući metode za upravljanje sistemom zaštite i bezbednosnim rizikom; razvoj i implementaciju programa, plana, politika i procedura zaštite; nadzor, kontrolu i reviziju sistema zaštite; upravljanje kompjuterskim incidentom, vanrednim događajem, fizičkom i personalnom zaštitom, obukom i obrazovanjem u zaštiti i sertifikacijom i akreditacijom sistema zaštite.

U dvanaest priloga date su liste relevantnih standarda zaštite, brojni primeri bezbednosne kategorizacije, malicioznih programa, ranjivosti i pretnji IKT sistema, kao i grafički modeli konfigurisanja logičkih barijera u računarskoj mreži i metodi procene ukupnog bezbednosnog rizika.

Autori se zahvaljuju recenzentima prof. dr Milanu Stanišiću i prof. dr Branku Kovačeviću na korisnim sugestijama, lektoru Snježani Krstić na pravopisnim ispravkama, Aleksandru Mihajloviću na dizajnu korica i Novaku Njegušu na prelomu i tehničkoj obradi ovog udžbenika.



SADRŽAJ

UVOD XV

GLAVA I
BEZBEDNOST INFORMACIONIH SISTEMA

1. BEZBEDNOST I ZAŠTITA INFORMACIJA 3
1.1. UVOD 3
1.2. BEZBEDNOST INFORMACIJA 4
1.2.1. Definicije pojmova bezbednost i sigurnost informacija 4
1.2.2. Funkcionalna zavisnost bezbednost – pretnje 6
1.2.3. Glavni faktori uticaja na bezbednosno stanje ikts 7
1.3. OPŠTA DEFINICIJA SISTEMA ZAŠTITE 9
1.3.1. Osnovne funkcionalnosti sistema zaštite 10
1.3.2. Informacioni sistem kao objekat zaštite 11
1.3.3. Generički, funkcionalni model sistema zaštite 13
1.3.4. Definisanje optimalnog sistema zaštite 14
1.3.5. Promena paradigme zaštite ikts i informacija 16
1.3.6. Opšti metod implementacije sistema zaštite 18
1.4. REZIME 22
1.5. KLJUČNI TERMINI 24
1.6. PITANJA ZA PONAVLJANJE 25

2. PRINCIPI, STANDARDI I NORMATIVI ZAŠTITE 28
2.1. UVOD 28
2.2. SISTEMSKI PRINCIPI ZAŠTITE 29
2.3. OPŠTE PRIHVAĆENI PRINCIPI ZAŠTITE 30
2.3.1. Namena gaisp principa zaštite 30
2.3.2. Struktura GAISP principa zaštite 30
2.3.2.1. Opšti GAISP principi zaštite 31
2.3.2.2. Funkcionalni GAISP principi zaštite 32
2.3.2.3. Detaljni GAISP principi zaštite 32
2.4. STANDARDI ZAŠTITE 33
2.4.1. Generička definicija standarda zaštite 33
2.4.2. Opšti model standarda zaštite 33
2.4.3. Tela za standardizaciju zaštite 34
2.4.4. Klasifikacija standarda zaštite 35

2.4.5. Prednosti i nedostaci standarda zaštite 37
2.5. NORMATIVNI OKVIR ZAŠTITE 37
2.6. DOKUMENTACIJA ZAŠTITE 38
2.7. REZIME 40
2.8. KLJUČNI TERMINI 41
2.9. PITANJA ZA PONAVLJANJE 41

3. METODOLOGIJE, MODELI I OKVIRI SISTEMA ZAŠTITE 44
3.1. UVOD 44
3.2. METODOLOŠKI OKVIRI ZA RAZVOJ SISTEMA ZAŠTITE 44
3.3. MODELOVANJE SISTEMA ZAŠTITE 47
3.3.1. Strukturni modeli distribuiranog IKT sistema 47
3.3.2. Objektno orijentisano modelovanje sistema zaštite 49
3.4. REZIME 52
3.5. KLJUČNI TERMINI 52
3.6. PITANJA ZA PONAVLJANJE 53

4. KONCEPTI SISTEMA ZAŠTITE 54
4.1. UVOD 54
4.2. KONCEPT SISTEMA REAKTIVNE ZAŠTITE 54
4.2.1. Sistem reaktivne zaštite 54
4.2.1.1. Funkcionalni model reaktivne zaštite 55
4.2.1.2. Ocena kvaliteta sistema reaktivne zaštite 56
4.3. KONCEPT SISTEMA PROAKTVNE ZAŠTITE 57
4.3.1. Funkcionalni model proaktivne zaštite 58
4.4. KONCEPT KONTROLA ZAŠTITE 61
4.4.1. Osnovne karakteristike kontrola zaštite 61
4.4.2. Skup kontrola za sistem osnovne zaštite 63
4.4.3. Proces selekcije i implementacije kontrola zaštite 64
4.4.4. Procena efektivnosti kontrola zaštite 66
4.4.5. Dokumentovanje kontrala zaštite u planu zaštite 67
4.5. REZIME 67
4.6. KLJUČNI TERMINI 68
4.7. PITANJA ZA PONAVLJANJE 68

5. OPŠTI MODEL SERVISA ZAŠTITE 71
5.1. UVOD 71
5.2. SERVISI ZAŠTITE 72
5.2.1. Misija i ciljevi sistema zaštite 72
5.2.2. Međuzavisnost bezbednosnih ciljeva 73
5.3. OPŠTI MODEL SERVISA ZAŠTITE 74
5.4. RAZVOJ I IMPLEMENTACIJA SERVISA ZAŠTITE 80
5.4.1. Isporuka servisa zaštite 80
5.5. REZIME 81

5.6. KLJUČNI TERMINI 81
5.7. PITANJE ZA PONAVLJANJE 82

6. METRIČKI SISTEMI ZAŠTITE INFORMACIJA 84
6.1. UVOD 84
6.2. METODOLOGIJA METRIKE SISTEMA ZAŠTITE INFORMACIJA 84
6.2.1. Definicije pojmova 84
6.2.2. Principi, namena, program i procesi metričkog sistema 85
6.2.3. Osnovne karakteristike metrika zaštite informacija 88
6.2.4. Procesno orijentisani metrički sistemi 89
6.2.5. Izbor tipa i razlozi za primenu metrika zaštite 91
6.2.6. Primeri metričkih sistema operativnih kontrola zaštite 92
6.2.7. Prezentovanje metrika zaštite informacija 93
6.2.8. Prednosti i nedostaci metričkih sistema zaštite 95
6.3. REZIME 96
6.4. KLJUČNI TERMINI 97
6.5. PITANJA ZA PONAVLJANJE 97

7. TAKSOMOMIJA PRETNJI I MALICIOZNIH PROGRAMA 100
7.1. UVOD 100
7.2. PRETNJE I NAPADI 100
7.2.1. Taksonomije pretnji i napada 100
7.3. PREGLED MALICIOZNIH PROGRAMA 105
7.3.1. Osnovne vrste savremenih malicioznih programa 105
7.3.2. Taksonomija virusa 106
7.3.2.1. Mehanizmi širenja virusa 108
7.3.3. Karakteristike crva 110
7.3.4. Kombinovani napad 111
7.3.5. Trojanci i ostali maliciozni programi 112
7.3.6. Metodi skrivanja malicioznih programa 114
7.4. DISTRIBUCIJA MALICIOZNIH PROGRAMA 116
7.5. MERE ZAŠTITE I OPORAVAK SISTEMA OD MALICIOZNIH NAPADA 120
7.6. REZIME 122
7.7. KLJUČNI TERMINI 123
7.8. PITANJA ZA PONAVLJANJE 123

8. TEHNOLOGIJE ZA ZAŠTITU RAČUNARSKIH SISTEMA 127
8.1. UVOD 127
8.2. KLASIFIKACIJA ALATA ZA ZAŠTITU 127
8.3. MEHANIZMI ZAŠTITE RAČUNARSKOG SISTEMA 129
8.3.1. Apstraktni bezbednosni slojevi računarskog sistema 129
8.3.2. Podsistem za zaštitu os (nosss) 130
8.3.3. Logička kontrola pristupa računarskom sistemu 131
8.3.3.1. *Mehanizmi logičke kontrole pristupa* 132

8.3.3.2. *Univerzalni mehanizmi logičke kontrole pristupa* 134
8.3.4. Zaštita integriteta računarskog sistema 135
8.3.5. Mehanizmi za detekciju i sprečavanje upada u sistem 139
8.3.6. Mehanizmi za zaštitu poverljivosti i integriteta podataka 140
8.3.6.1. Osnovi kriptografije - simetrični šifarski sistemi 142
8.3.6.2. Osnovi kriptografije – asimetrični šifarski sistemi 143
8.4. REZIME 145
8.5. KLJUČNI TERMINI 147
8.6. PITANJA ZA PONAVLJANJE 147

9. TEHNOLOGIJE ZA ZAŠTITU RAČUNARSKIH MREŽA 150
9.1. UVOD 150
9.2. SERVIS LOGIČKE KONTROLE PRISTUPA RAČUNARSKOJ MREŽI 150
9.2.1. Mehanizmi logičke kontrole pristupa računarskoj mreži 150
9.2.1.1. Logičke mrežne barijere 151
9.2.1.2. Proksi serveri 153
9.2.1.3. Web filteri 153
9.2.1.4. Autentifikacioni protokoli 154
9.2.1.5. Serveri za autentifikaciju i autorizaciju 157
9.2.1.6. Smart kartice i kriptografski moduli 159
9.2.1.7. Ostali autentifikacioni uređaji i protokoli 160
9.2.2. Zaštita integriteta računarske mreže 162
9.2.2.1. Skeneri ranjivosti računarske mreže 162
9.2.2.2. Skeneri telefonskih veza 165
9.2.3. Mehanizmi za detekciju i sprečavanje upada u mrežu 166
9.2.4. Infrastrukturni mehanizmi za zaštitu računarske mreže 168
9.2.4.1. Infrastruktura sa javnim ključem 168
9.2.4.2. IPSec protokol 173
9.2.5. Bezbednost bežičnih lokalnih mreža 177
9.3. REZIME 181
9.4. KLJUČNI TERMINI 183
9.5. PITANJA ZA PONAVLJANJE 183
9.6. LITERATURA 186

GLAVA II
UPRAVLJANJE SISTEMOM ZAŠTITE INFORMACIJA

1. UPRAVLJANJE ZAŠTITOM INFORMACIJA 193
1.1. UVOD 193
1.2. METODOLOŠKI OKVIR ZA UPRAVLJANJE ZAŠTITOM 194
1.2.1. Principi upravljanja zaštitom 194
1.2.2. Uloge i odgovornosti 194
1.2.3. Generički proces upravljanja zaštitom informacija 195
1.2.4. Sistem upravljanja zaštitom informacija. 197

1.2.4.1. Uspostavljanje ISMS *198*
1.2.4.2. Administracija sistema zaštite 200
1.2.4.3. Metrika za evaluaciju upravljanja sistemom zaštite 200
1.2.5. Otvoreni problemi upravljanja zaštitom informacija 201
1.2.6. Preporuke za upravljanje zaštitom informacija 202
1.3. REZIME 205
1.4. KLJUČNI TERMINI 205
1.5. PITANJA ZA PONAVLJANJE 206

2. UPRAVLJANJE BEZBEDNOSNIM RIZIKOM **209**
2.1. UVOD 209
2.2. OPŠTA METODOLOGIJA ZA UPRAVLJANJE RIZIKOM 210
2.2.1. Glavni principi upravljanja rizikom 210
2.2.2. Generički metod kvalitativne procene rizika 213
2.2.3. Formalna metodologija za procenu rizika 214
2.2.3.1. Uspostavljanje konteksta za procenu rizika *216*
2.2.3.2. Proces analize i evaluacije rizika *218*
2.2.3.3. Modeli procena ukupnog bezbednosnog rizika *228*
2.3. REZIME 229
2.4. KLJUČNI TERMINI 230
2.5. PITANJA ZA PONAVLJANJE 231

3. UPRAVLJANJE PROGRAMOM ZAŠTITE INFORMACIJA **234**
3.1. UVOD 234
3.2. RAZVOJ I STRUKTURA PROGRAMA, PLANA I POLITIKE ZAŠTITE 235
3.2.1. Struktura programske politike zaštite 235
3.2.2. Razvoj i struktura plana zaštite 235
3.2.2.1. Uloge i odgovornosti *236*
3.2.2.2. Upravljanje promenama *237*
3.2.3. Razvoj i struktura politike i procedura zaštite 237
3.2.3.1. Struktura i taksonomija politike zaštite *238*
3.2.3.2. Razvoj politike zaštite *241*
3.2.3.3. Razvoj procedura zaštite *245*
3.3. PREPORUČENA DOKUMENTACIJA ZA IMPLEMENTACIJU ISMS 246
3.4. USPOSTAVLJANJE UPRAVLJAČKOG OKVIRA SISTEMA ZAŠTITE 248
3.5. REZIME 250
3.6. KLJUČNI TERMINI 251
3.7. PITANJA ZA PONAVLJANJE 252

4. NADZOR, KONTROLA I REVIZIJA SISTEMA ZAŠTITE **255**
4.1. UVOD 255
4.2. PROCESI NADZORA, KONTROLE I REVIZIJE SISTEMA ZAŠTITE 255
4.2.1. Glavni aspekti procesa kontrole i revizije sistema zaštite 256
4.2.2. Planiranje nadzora, kontrole i revizije sistema zaštite 257

4.3. REZIME 261
4.4. KLJUČNI TERMINI 262
4.5. PITANJA ZA PONAVLJANJE 262

5. UPRAVLJANJE KOMPJUTERSKIM INCIDENTOM I VANREDNIM DOGAĐAJEM 264
5.1. UVOD 264
5.2. KOMPJUTERSKI DOGAĐAJ I KOMPJUTERSKI INCIDENT 265
5.2.1. Politika i procedure za upravljanje incidentom 265
5.2.2. Kategorije bezbednosnog kompjuterskog incidenta 265
5.2.3. Nagoveštaji kompjuterskog incidenta 266
5.2.4. Upravljanje kompjuterskim incidentom 266
5.3. PLANIRANJE VANREDNIH DOGAĐAJA U IKTS 269
5.4. REZIME 275
5.5. KLJUČNI TERMINI 276
5.6. PITANJA ZA PONAVLJANJE 277

6. UPRAVLJANJE FIZIČKO - TEHNIČKOM ZAŠTITOM 281
6.1. UVOD 281
6.2. STANDARDI FIZIČKE ZAŠTITE 281
6.2.1. Standardi fizičke zaštite za računarsku sobu i radne stanice 281
6.3. FIZIČKA ZAŠTITA I ZAŠTITA OKRUŽENJA IKTS 282
6.3.1. Rizici proboja fizičke zaštite i zaštite okruženja ikts 282
6.3.2. Fizička zaštita IKTS i okruženja 282
6.3.3. Zaštita EM i optičkih medija 284
6.3.4. Metodi uništavanja medija 286
6.3.5. Kriterijumi za izbor i implementaciju fizičke zaštite 287
6.3.6. Sistemi zaštite okruženja ikts 287
6.4. KONVERGENCIJA FIZIČKE I LOGIČKE KONTROLE PRISTUPA 288
6.5. REZIME 290
6.6. KLJUČNI TERMINI 291
6.7. PITANJA ZA PONAVLJANJE 291

7. UPRAVLJANJE PERSONALNOM ZAŠTITOM 294
7.1. UVOD 294
7.2. PROCES POPUNE RADNIH MESTA U IKTS 294
7.2.1. Određivanje osetljivosti radnog mesta 295
7.2.2. Popuna radnih mesta i izbor zaposlenih 295
7.2.3. Obuka zaposlenih 296
7.3. UPRAVLJANJE KORISNIČKIM NALOZIMA 296
7.3.1. Revizija prakse upravljanja korisničkim nalozima 297
7.3.2. Detekcija nelegalnih aktivnosti zaposlenih 298
7.3.3. Privremena zamena i interni transfer zaposlenih 298
7.3.4. Ukidanje naloga 298
7.3.5. Personalna zaštita spoljnih saradnika po ugovoru 299

7.3.6. Personalna zaštita u ikts sa javnim pristupom 299
7.3.7. Uspostavljanje tima za zaštitu informacija 300
7.4. REZIME 301
7.5. KLJUČNI TERMINI 301
7.6. PITANJA ZA PONAVLJANJE. 301

8. UPRAVLJANJE OBUKOM I OBRAZOVANJEM U ZAŠTITI 304
8.1. UVOD 304
8.2. RAZVOJ SVESTI, OBUKA I OBRAZOVANJE U ZAŠTITI 304
8.2.1. Program za razvoj svesti o potrebi zaštite 305
8.2.2. Program obuke u zaštiti 306
8.2.3. Obrazovanje u zaštiti 306
8.2.4. Kontinuitet procesa obrazovanja u zaštiti 307
8.2.5. Znanje i veštine članova tima za upravljanje zaštitom 308
8.3. UPRAVLJANJE PROGRAMOM OBUKE U ZAŠTITI 309
8.4. PROCES RAZVOJA PROGRAMA OBUKE U ZAŠTITI 311
8.5. REZIME 313
8.6. KLJUČNI TERMINI 314
8.7. PITANJA ZA PONAVLJANJA 314

9. SERTIFIKACIJA I AKREDITACIJA SISTEMA ZAŠTITE 316
9.1. UVOD 316
9.2. ORGANIZACIJA PROCESA SERTIFIKACIJE I AKREDITACIJE 316
9.2.1. Uloge i odgovornosti 316
9.3. UPRAVLJANJE PROCESOM SERTIFIKACIJE I AKREDITACIJE 318
9.3.1. Sertifikaciona i akreditaciona dokumentacija 321
9.3.2. Tipovi i proces akreditacije 322
9.3.3. Faza post–akreditacije 325
9.4. REZIME 326
9.5. KLJUČNI TERMINI 327
9.6. PITANJA ZA PONAVLJANJE 327
9.7. LITERATURA 330

PRILOZI
PRILOG 1: ISO 27K STANDARDI – OBJAVLJENI ILI U TOKU IZRADE 337
PRILOG 2: RELEVANTNI STANDARDI ZAŠTITE 338
PRILOG 3: PRIMER BEZBEDNOSNE KATEGORIZACIJE OBJEKATA VELIKOG IKTS 343
PRILOG 4: METOD POKRIVANJA PRETNJI KONTROLAMA ZAŠTITE 345
PRILOG 5: KRATKA ISTORIJA MALICIOZNIH PROGRAMA 347
PRILOG 6: PRIMERI KONFIGURACIJE LOGIČKE BARIJERE U RAČUNARSKOJ MREŽI 348
PRILOG 7: GRAFIČKI MODEL IMPLEMENTACIJE ISMS 350
PRILOG 8: TIPIČNI PAROVI RANJIVOSTI/PRETNJA (T/V) 351
PRILOG 9: TIPOVI UOBIČAJENIH PRETNJI (ISO/IEC 27005) 355
PRILOG 10: PRIMERI ODREĐIVANJA VEROVATNODE I NEODREĐENOSTI PRETNJI 360
PRILOG 11: METODI PROCENE UKUPNOG RIZIKA 365
PRILOG 12: KONTROLNA LISTA PROCESA IMPLEMENTACIJE POLITIKE I PROCEDURA ZAŠTITE 370

SPISAK SLIKA

GLAVA I

Slika 1.1 Nivo ukupne bezbednosti u funkciji komponenti bezbednosti
Slika 1.2 Nivo ukupne bezbednosti IKTS u funkciji pretnji
Slika 1.3 Generički model sistema zaštite i međusobni odnosi komponenti
Slika 1.4 Optimalni sistem zaštite informacija
Slika 2.1 Opšti model standarda zaštite informacija [61]
Slika 2.2 Organizaciona šema Tehničkog komiteta ISO/IEC JTC 1SC 27
Slika 2.3 Klasifikacija standarda zaštite
Slika 2.4 Klasifikacija dokumentacije zaštite
Slika 3.1 Strategija bezbednosti IKTS u funkciji sistema zaštite
Slika 3.2 Izlaz modelovanja sistema osnovne zaštite IKTS
Slika 4.1 Funkcionalni model sistema reaktivne zaštite
Slika 4.2 Vremenski prozori proaktivnih i reaktivnih sistema zaštite [53]
Slika 4.3 Procenat otkrivanja ranjivosti IKTS u periodu 1998–2005 [53]
Slika 4.4 Zona – (a) i proširеni vremenski prozor proaktivne zaštite- (b) [53]
Slika 5.1 Međuzavisnost bezbednosnih ciljeva
Slika 5.2 Opšti model servisa zaštite
Slika 5.3 Primarni servisi za zaštitu raspoloživosti
Slika 5.4 Primarni servisi za zaštitu integriteta
Slika 5.5 Primarni servisi za zaštitu poverljivosti
Slika 5.6 Distribuirani servisi zaštite
Slika 5.7 DMZ sa jednom barijerom – (a) i dve barijere – (b) [85]
Slika 6.1 Struktura – (a) i proces programa – (b) metričkog sistema zaštite informacija
Slika 6.2 Sazrevanje tehnologija zaštite
Slika 6.3 Uloge kojima se najčešće prezentuju metrike zaštite u organizaciji
Slika 6.4 Primeri metoda za prezentovanje metrike zaštite informacija
Slika 7.1 Generička taksonomija napada
Slika 7.2 Generički tok napada na računarske mreže i sisteme
Slika 7.3 Ključni tipovi incidenata izraženi u procentima (2008) [96]
Slika 7.4 Zastupljenost malicioznih napada u 2009 godini [96]
Slika 7.5 Prikaz neinficiranog i inficiranog boot sektora
Slika 7.6 Dopisivanje ispred izvršne datoteke
Slika 7.7 Dopisivanje na kraju izvršne datoteke
Slika 7.8 Generička struktura crva
Slika 7.9 Najčešće korišćene tehnike samozaštite malicioznih programa [111]
Slika 7.10 Države koje hostuju najviše zlonamernih programa [116]
Slika 7.11 Razvoj malicioznih programa (*malvera*) u periodu 2003-2010.
Slika 7.12 Države iz kojih se šalje najviše spam poruka [116]
Slika 7.13 Pad količine SPAM poruka tokom 11.10.2008. godine [116]
Slika 7.14 Pregled efektivnosti antivirusnih programa u 2009 godini [32]

Slika 8.1 Klasifikacija alata za zaštitu
Slika 8.2 Apstraktni bezbednosni slojevi RS
Slika 8.3 Generički servis logičke kontrole pristupa
Slika 8.4 Mehanizmi logičke kontrole pristupa [62]
Slika 8.5 Faze procesa upravljanja ranjivostima
Slika 8.6 Primena skenera ranjivosti u IKTS srednje veličine
Slika 8.7 IDPS koncept
Slika 8.8 Komunikacija sa šifrovanjem podataka
Slika 8.9 Sadržaj standardnog ITU X.500 DS-3-0
Slika 8.10 Zavisnost mehanizama zaštite od vrednosti imovine i izloženosti
Slika 9.1 Tok procesa filtriranja paketa
Slika 9.2 Principi rada filterskih i aplikativnih barijera
Slika 9.3 Zaštita perimetra računarske mreže sa dve barijere [19]
Slika 9.4 Konfiguracija aplikativnog proksija [19]
Slika 9.5 Lokacija SSL protokola u višeslojnoj arhitekturi RM
Slika 9.6 Funkcionalni model RADIUS protokola
Slika 9.7 Upotreba kriptokartice sa eksternim čitačem kartica
Slika 9.8 Tipičan skener za procenu ranjivosti RS – (a) i implementacija u RM – (b) [109]
Slika 9.9 Rezultat pingovanja mrežnih uređaja u Nmap alatu (PingSweep)
Slika 9.10 Skeneri ranjivosti računarskih mreža
Slika 9.11 Rezultati analize ranjivosti – (a) i tipovi izveštaja – (b) u Retina alatu
Slika 9.12 Glavne ranjivosti RM (2006) [60]
Slika 9.13 Linearna aproksimacija rasta ranjivosti od 2000–2006 [60]]
Slika 9.14 Mogućnosti primene NIDPS sistema u RM [87]
Slika 9.15 Upravljanje NIDPS sistemima: centralizovano – (a) i distribuirano – (b) [87]
Slika 9.16 Ključni moduli PKI sistema
Slika 9.17 Model globalne arhitekture PKI sistema
Slika 9.18 Struktura paketa podataka za prenos putem Ethernet mreža: IP – (a) i IPSec – (b)
Slika 9.19 Struktura IPSec paketa podataka uz korištenje AH potprotokola u Ethernet mreži
Slika 9.20 Struktura IPSec paketa uz korištenje ESP potprotokola u Ethernet mrežama
Slika 9.21 Funkcionalni model WEP protokola
Slika 9.22 Princip rada 802.11i u četiri faze

GLAVA II

Slika 1.1 Generički proces ISMS – (a) i usaglašenosti sa BS – (b)
Slika 1.2 PDCA (Plan, Do, Check Act) model
Slika 1.3 Primena PDCA modela na ISMS prema ISO/IEC 27001
Slika 1.4 Skala sazrevanja procesa upravljanja
Slika 2.1 Model – (a) i hijerarhijski pristup upravljanju – (b) strateškim rizikom
Slika 2.2 Generički okvir – (a) i ciklus – (b) upravljanja rizikom
Slika 2.3 Generički model za analizu i procenu rizika [67]

Slika 2.4 Tok procesa UR od namernog, nemalicioznog eksternog napada
Slika 2.5 Dijagram odnosa „uticaj–verovatnoća neuspeha“ napada
Slika 2.6 Funkcionalni model procesa procene rizika
Slika 2.7 Implementirane kontrole zaštite i preostali rizik–Rrp
Slika 3.1 Generički proces razvoja plana zaštite
Slika 3.2 Funkcionalni model za razvoj politike zaštite
Slika 3.3 Ciklus procesa održavanja politike zaštite
Slika 3.4 Klasifikacija dokumenata zaštite
Slika 3.5 Sazrevanje procesa upravljačkog okvira zaštite
Slika 5.1 Životni ciklus – (a) procesa upravljanja bezbednosnim incidentom – (b)
Slika 5.2 Dijagram troškova bekapovanja i vremena oporavka u funkciji rezervne lokacije
Slika 6.1 Tok procesa saniranja i odlaganja dokumenata i medija
Slika 6.2 Model odnosa logičke i fizičke kontrole pristupa [35]
Slika 7.1 Proces popune zaposlenih u IKT sistemu
Slika 8.1 Model kontinuiteta procesa učenja i osposobljavanja u zaštiti
Slika 8.2 Centralizovano – (a) i delimično decentralizovano – (b) upravljanje programom obuke
Slika 8.3 Decentralizovano upravljanje programom obuke u zaštiti
Slika 8.4 Evaluacija i tehnike povratne sprege za kontrolu programa
Slika 9.1 Faze i aktivnosti procesa sertifikacije i akreditacije [1]
Slika 9.2 Plan sertifikacije sistema zaštite [1]
Slika 9.3 Akreditacija sistema – (a) i tipska akreditacija – (b) [1]
Slika 9.4 Lokacijska akreditacija [1]

SPISAK TABELA

GLAVA I

Tabela 1.1 Klasifikacija informacione imovine
Tabela 1.2 Relevantni aspekti zaštite IKTS
Tabela 1.2 Faze implementacije sistema zaštite
Tabela 2.1 Opšti GAISP principi zaštite
Tabela 2.2 Relevantna međunarodna tela za standardizaciju u oblasti zaštite
Tabela 2.3 Primeri dokumentacije zaštite
Tabela 3.1 Ključni koncepti za razvoj sistema zaštite
Tabela 4.1 Klase, familije i identifikatori kontrola zaštite
Tabela 4.2 Dimenzije kontrola zaštite
Tabela 4.3 Primer matrice praćenja zahteva za zaštitom
Tabela 4.4 Metodi za procenu efektivnosti kontrola zaštite za različite nivoe uticaja
Tabela 6.1 Pristup za izbor metrike – odozgo nadole
Tabela 6.2 Pristup za izbor metrike – odozdo nagore

Tabela 6.3 Karakteristike metrika zaštite informacija
Tabela 6.4 Primeri metrika zaštite prema kategorijama
Tabela 6.5 Najčešće korišćene metrike zaštite informacija
Tabela 6.6 Istraživanja primene metrika zaštite informacija u praksi
Tabela 7.1 Zbirne karakteristike atributa namernih napada
Tabela 7.2 Pomeranje vektora napada sa Interneta
Tabela 7.3 Uporedne karakteristike nekih malicioznih programa
Tabela 8.1 Statistika korisničke upotrebe lozinke
Tabela 8.2 Primer proračuna prozora poznatih ranjivosti
Tabela 8.3 Kriterijumi procene vrednosti kriptološkog algoritma
Tabela 8.4 Vrednovanje kriptoloških algoritama za mehanizme zaštite
Tabela 9.1 Mrežni protokoli sa poznatim ranjivostima
Tabela 9.2 Kriptografski algoritmi za komunikaciju SSL protokolom
Tabela 9.3 Autentiikacioni i autorizacioni protokoli
Tabela 9.4 Zbirne prednosti instalacija NIDS na različitim lokacijama u RM
Tabela 9.5 Funkcionalnosti CA i RA
Tabela 9.6 Servisi i mehanizmi mrežne zaštite
Tabela 9.7 Standardni tipovi bežičnih mreža
Tabela 9.8 Osnovne karakteristike protokola zaštite WLAN sistema
Tabela 9.9 Uporedne vrednosti funkcija protokola zaštite WLAN sistema

GLAVA II

Tabela 1.1 Glavni principi upravljanja rizikom
Tabela 2.1 Primer intuitivne procene atributa A,V,T i relativnog rizika (Rr)
Tabela 2.2 Kriterijumi za određivanje težinskih faktora vrednosti A
Tabela 2.3 Primer procene relevantnih faktora ranjivosti (V)
Tabela 2.4 Primeri tipova kombinovanih pretnji
Tabela 2.5 Proračun težinskih faktora za verovatnoću pojave incidenta
Tabela 2.6 Kriterijumi za ponderisanje intenziteta potencijalnih pretnji
Tabela 2.7 Kriterijumi za određivanje težinskih faktora frekvencije incidenta
Tabela 2.8 Komponente za određivanje težinskih faktora uticaja rizika
Tabela 3.1 Glavni principi za razvoj politike zaštite
Tabela 3.2 Bezbednosne kategroije upravljačkog okvira sistema zaštite
Tabela 3.3 Kapaciteti procesa upravljačkog okvira po nivoima zrelosti
Tabela 4.1 Ciljevi i metrike kontrole i revizije sistema zaštite
Tabela 6.1 Standard stepena saniranja ključnih kategorija medija
Tabela 7.1 Osnovna podela zadataka u timu za upravljanje zaštitom informacija
Tabela 7.2 Proširene uloge u timu za zaštitu u praksi zaštite
Tabela 8.1 Komparacija parametara svesti o potrebi, obuke i obrazovanja u zaštiti
Tabela 8.2 Znanja i veštine članova tima za zaštitu informacija
Tabela 9.1 Tehnike verifikacije za nivoe bezbednosne sertifikaciju

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM



UVOD

Produktivnost savremenih poslovnih sistema u najvećoj meri zavisi od brzine donošenja odluka i kvaliteta upravljanja. Odlučivanje, a time i kvalitet upravljanja u potpunosti zavise od *kvaliteta informacija*, koje procesiraju, skladište i prenose računarski sistemi (RS) i računarske mreže (RM). U ovom udžbeniku umesto uobičajenih skraćenica IS (Informacioni sistem) ili IT (informacione tehnologije) koristiće se termin *sistem informaciono komunikacionih tehnologija* (IKTS), koji generički uključuje sve atribute i aspekte bezbednosti i zaštite: *sistemski* pristup, *informacione objekte* (informacije, podatke, programe), *tehnologije* (mrežne, informacione, komunikacione, zaštite) i *ljude*. Takođe, termin *zaštita informacija* implicira *zaštitu IKTS* u celini, pa se ova dva termina u udžbeniku koriste ravnopravno.

U skladu sa objektno - orijentisanim pristupom, od brojnih atributa informacija, kvalitet informacija u potpunosti zavisi od skupa relativno nezavisnih atributa: *poverljivosti* – da informacije nisu otkrivene neovlašćenim korisnicima; *integriteta* – da informacije nisu neovlašćeno izmenjene i *raspoloživosti* – da su informacije dostupne legitimnim korisnicima kada je to potrebno. Kvalitet procesiranih, skladištenih i prenošenih informacija u savremenim visoko distribuiranim i umreženim IKTS Internet tipa, zavisi od funkcionalne pouzdanosti i bezbednosti sistema i njegovog okruženja, odnosno, od implementiranog sistema zaštite. Na taj način, pored kvaliteta *hardvera* i *softvera, bezbednost* IKTS postaje treći gradivni blok sistema kvaliteta poslovnih IKTS i poslovnih sistema u celini.

Udžbenik *Osnove zaštite informacija,* namenjen je studentima osnovnih studija, ali i korisnicima i menadžerima koji prvi put ulaze u problematiku zaštite informacija. Mogu ga koristiti i profesionalci u zaštiti koji žele sistematizovati i upotpuniti svoja zna-nja iz ove široke, multidisciplinarne oblasti.

Glavni cilj pisanja ovog udžbenika je da se raznovrsna i obimna teorija, dostupna u brojnoj stranoj literaturi, stručnim časopisima, preporukama, uputstvima, standardima i autorskim radovima na Internetu, sistematizuje, terminološki ujednači i definiše i što više približi korisnicima i menadžerima, koji po pravilu ne moraju biti tehnički obrazovani. Smanjenje kompleksnosti terminologije zaštite jedan je od strateških ciljeva teorije i prakse zaštite. Time se postiže veća razumljivost i korisnička prihvatljivost zaštite.

Metodološki, udžbenik je koncipiran u dve glave: *Metodološko tehnološke osnove zaštite IKTS i Upravljanje zaštitom IKTS,* sa ukupno osamnaest poglavlja. Svako poglavlje je koncipirano modularno sa uvodom, razradom razmatranog problema zaštite, rezimeom (kratkim sadržajem), ključnim terminima i pitanjima za ponavljanje. Spisak korišćene i šire literature dat je na kraju svake glave.

Sa metodološkog aspekta, za obradu celokupne problematike zaštite u zadatom okviru udžbenika korišćeni su i razmatrani sledeći ključni koncepti:

1. *koncept terminologije zaštite,* kao jedan od glavnih ciljeva udžbenika, primenjen je u svakom poglavlju sa posebnim definisanjem ključnih termina na kraju poglavlja;
2. k*oncept strateškog* (dugoročnog) i *taktičkog* (kratkoročnog) rešavanja problema bezbednosti i zaštite IKTS (planiranja i razvoja programa, plana i sistema zaštite);
3. k*oncept reaktivnih,* tradicionalnih sistema zaštite koji štite informacije i objekte IKTS od poznatih pretnji i *proaktivnih sistema zaštite* koji štite informacije od poznatih i nepoznatih, promenljivih, kombinovanih pretnji;
4. k*oncept sistemskog i procesnog pristupa,* kojim se definišu i identifikuju upravljački, operativno - organizacioni i tehnički procesi i kontrole zaštite. Sistemski i procesni pristup zaštiti značajan je i zato što obezbeđuje osnovu za dalji rad u ovoj oblasti i omogućava projektantima IKTS i sistema zaštite da lakše usklade razvoj životnih ciklusa IKTS i sistema zaštite sa bolje definisanim procesima i metodima, što u praksi najčešće nije slučaj (sistem zaštite se uglavnom implementira pri kraju ili posle razvoja životnog ciklusa IKTS);
5. k*oncept objektno orijentisanog* modelovanja (OOM) IKTS kao objekta zaštite i sistema zaštite kao sredstava za zaštitu, primenjen je u udžbeniku u cilju smanjenja kompleksnosti IKTS i sistema zaštite. Opisana je primena OOM u oblasti zaštite i identifikovane su dve ključne grane objekata: *grana objekata zaštite – poverljivost, integritet i raspoloživost informacija* i *grana sredstava za zaštitu (objekata za zaštitu*) – *upravljačke, operativne i tehničke kontrole zaštite*. Razmatrane su

primene i ostalih atributa OOM na oblast zaštite: *klase*, *objekti*, *komponente objekta, kontejner*, *inkapsulacija, polimorfizam, nasleđivanje i dekompozicija.* Primena koncepta OOM na oblast zaštite ima višestruki značaj, a posebno treba istaći da se problematika zaštite na elegantan način dovodi u fokus vlasnika i projektanata IKTS, koji sada mogu istom metodologijom blagovremeno uskladiti razvoje životnih ciklusa IKTS i sistema zaštite. Na kraju su razmatrani neki koncepti *nove paradigme zaštite* sevisno orijentisanih *web* aplikacija – SOA (*Service Oriented Application*) i distribuiranog Internet računarstva (*Cloud Computing*).

U **Glavi I** definisani su i opisani u devet poglavlja: bezbednost, zaštita, sistem zaštite i optimalna zaštita; opšte prihvaćeni principi (GAISP, OECD, NIST), relevantni standardi (ISO/IEC 27001/2/5; ISO/IEC 21827 ili SSE CMM – *System Security Engeneering Capability Maturity Model* i dr.) i normativi zaštite; metodologije i modeli sistema zaštite; koncepti *kontrola* i sistema *reaktivne* i *proaktivne* zaštite; opšti model servisa zaštite; metrički sistemi zaštite informacija; taksonomije pretnji i malicioznih programa; tehnologije za zaštitu računarskih sistema i tehnologije za zaštitu računarskih mreža.

U **Glavi II**: *Upravljanje zaštitom informacionih sistema,* u devet poglavlja detaljnije su razmatrane upravljačke i operativne komponente zaštite. Naime, u upravljačkim i operativnim kontrolama zaštite ljudski faktor je nezamenljiv i odlučujući, a dobra praksa zaštite potvrdila je da se najbolji rezultati u zaštiti postižu, ako se ove kontrole kombinuju i razvijaju i implementiraju jedinstveno. U teoriji i praksi zaštite proces upravljanja sistemom zaštite generalno je najslabije razvijen proces zaštite. U tom smislu, posebno su razmatrani procesi: upravljanja sistemom zaštite; upravljanja bezbednosnim i operativnim rizikom IKTS; upravljanje programom zaštite; nadzor, kontrola i revizija sistema zaštite; upravljanje kompjuterskim incidentom i vanrednim događajem; upravljanje fizičko–tehničkom i personalnom zaštitom; upravljanje obukom i obrazovanjem u zaštiti i evaluacijom kvaliteta sistema zaštite (sertifikacijom i akreditacijom).

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

Glava I

BEZBEDNOST INFORMACIONIH SISTEMA



UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

1. BEZBEDNOST I ZAŠTITA INFORMACIJA

Po završetku ovog poglavlja studenti će razumeti:

- *Značaj usvajanja terminologije zaštite*
- *Semantičko značenje termina «bezbednost» i «zaštita»*
- *Funkcionalnu zavisnosti «bezbednost -zaštita» i «bezbednost-pretnje»*
- *Definicije «sistema zaštite» i «optimalnog sistema zaštite»*
- *Opšti funkcionalni model sistema zaštite*
- *Ključne faktore bezbednosnog stanja IKT sistema*
- *Neke koncepte nove paradigme zaštite u savremenom web okruženju*

1.1. UVOD

Termini: *bezbednost informacija ili informaciona bezbednost,* primarno podrazumevaju bezbednost informacija i podataka u IKTS, a sekundarno - *bezbednost objekata računarskog sistema* (RS) i *računarske mreže* (RM), čime se posredno štite informacije. Ovakav pristup implicira da je krajnji cilj bezbednosti i zaštite – *zaštita informacija i podataka*, koja se direktno ili posredno postiže zaštitom *informacione imovine*[1]. U stranoj literaturi se koriste različiti termini (eng. *information security*; rus. *безопасност информации;* nem*. Informations–sicherheit),* a u ovom udžbeniku se ravnopravno koriste termini *bezbednost informacija i informaciona bezbednost*, koji *uvek* impliciraju bezbednost *informacione imovine* u celini. Ključni termini korišćeni u ovom udžbeniku definisani su na kraju svakog poglavlja, sa namerom da se kompleksnost terminologije *zaštite informacija* što više smanji i približi krajnjim korisnicima, a time povećaju korisnička prihvatljivost i svest o potrebi zaštite.

Bezbednost informacija od dinamički promenljivih, kombinovanih pretnji, u nebezbednom Internet okruženju, obezbeđuje *sistem zaštite*. Da bi se definisao rentabilan sistem zaštite, opisani su *strukturni i objektno orijentisani* modeli. Glavni cilj je usmeriti pažnju na *upravljanje rizikom* i izbor *kontrola zaštite* za ublažavanje rizika. Kako je *profil rizika* specifičan za svaku organizaciju, primena standarda *najbolje prakse zaštite informacija* ne daje uvek najbolje rezultate, pošto standard ne uzima u obzir specifične profile rizika organizacija. Dakle, *optimalni sistem* zaštite informacija znači rentabilan i adekvatan sistem zaštite za dato poslovno okruženje, profil rizika i ukupne troškove zaštite.

1 [1] *informaciona imovina* – u ISO/IEC 27001 obuhvata *informacije, hardver, softver i ljude.*

1.2. BEZBEDNOST INFORMACIJA

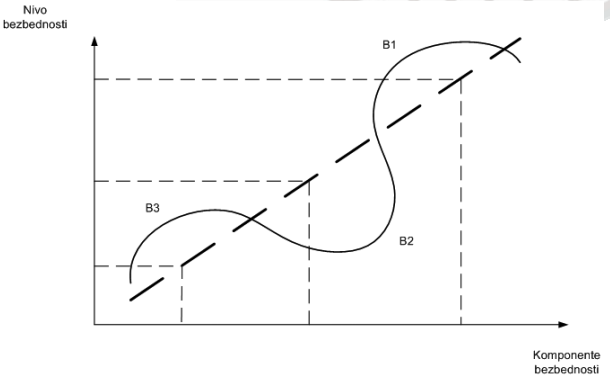
1.2.1. Definicije pojmova bezbednost i sigurnost informacija

U praksi zaštite postoje brojne definicije *bezbednosti informacija*, zavisno od nivoa apstrakcije. Na nivou države to je *stanje zaštićenosti nacionalnih interesa u informacionoj sferi, određenih skupom ličnih, poslovnih i državnih interesa*. Kako se bezbednost informacija obezbeđuje zaštitom, može se definisati i kao *zaštićenost informacija od slučajnih ili namernih aktivnosti prirodnog ili veštačkog karaktera, koje mogu naneti neprihvatljivu štetu informacionoj imovini organizacije* [21, 74, 61].

Bezbednost IKTS je *objektivna mera stanja rizika ili stanja bezbednog, pouzdanog i neometanog funkcionisanja sistema, u odnosu na samog sebe i svoje okruženje*. Sistem se smatra bezbednim, ako je *zaštićen* od uticaja faktora rizika. *Sigurnost* je sinonim *bezbednosti*, a semantički predstavlja *subjektivnu meru poverenja* ili osećaja sigurnosti da je sistem bezbedan. *Bezbednost sistema zaštite* semantički najbliže odgovara značenju engleskog termina *Security Assurance* (garantovana bezbednost).

Oba termina – *bezbednost* i *poverenje*, zasnivaju se na mehanizmu ljudske percepcije. IKTS se smatra objektivno *bezbednim,* ako je *do određenog stepena* pouzdano poznato da zaista poseduje neka bezbednosno relevantna svojstva, koja nominalno poseduje, a *siguran* je ili poverljiv, ako se *do određenog stepena veruje* da ima neka bezbednosno - relevantna svojstva koja nominalno poseduje. U oba slučaja termin *do određenog stepena* indicira relativnost definicija ovih pojmova.

U realnom okruženju, *bezbednost IKTS* je složen fenomen sa sociološko - kulturološkim i tehnološkim faktorima. Zato za ocenu *nivoa bezbednosnog stanja IKTS* treba uključiti sve ove aspekte. U opštem slučaju, ukupna bezbednost nekog složenog sistema obuhvata skup *komponenti bezbednosti (B1, B2...Bn)* (Sl. 1.1).



Sl. 1.1. Nivo ukupne bezbednosti u funkciji komponenti bezbednosti

Nivo ukupne bezbednosti sistema – **Bu** raste sa porastom nivoa bezbednosti njenih *relativno nezavisnih* bezbednosnih komponenti, čiji se skupovi negde presecaju, ali približno aditivno doprinose porastu ukupne bezbednosti. U idealnom

slučaju, da je bezbednost deterministička veličina, ova bi zavisnost bila linearna funkcija. Međutim, **Bu** je uvek *nelinearna funkcija* komponenti bezbednosti, zbog stohastičke prirode kombinovanih, dinamički promenljivih pretnji i neodređenosti faktora rizika, koji utiču na bezbednost [61].

Ukupna bezbednost složenog sistema – *Bu*, koja obuhvata sve komponente bezbednosti (*B1*,...*Bn*), može se izraziti *približnom* relacijom:

$$B_u = \sum_{j=1}^{n} k_j \cdot B_j$$

gde su:

$j=1,2,...,n$ – komponente bezbednosti, a

$k=1,2,...,k_n$ – težinski faktori uticaja pojedinačnih komponenti bezbednosti, koji različito doprinose porastu Bu.

Najveći uticaj na Bu, npr. države, imaju najosetljivije komponente – *državna, vojna, ekonomska i informaciona* bezbednost. Kako se razvija informatičko društvo, u toj meri raste značaj *informaciono - kibernetičke bezbednosti*[2], odnosno – *bezbednosti informacija,* koja prožima sve aspekte bezbednosti.

Uobičajeno se *bezbednost računarskih sistema* (RS), *mreža* (RM) ili IKTS poistovećuje sa *bezbednošću informacija*, jer u savremenom informacionom društvu informacija postaje najvrednija imovina organizacije. Osnovna razlika između bezbednosti informacija i bezbednosti RS/RM/IKTS je u pristupu i metodologiji zaštite. U objektno orijentisanom pristupu, bezbednost informacija se odnosi na zaštitu *poverljivosti, integriteta i raspoloživosti* – **CIA** (*Confidenciality, Integrity, Avialability*) informacija, bez obzira na formu u kojoj se informacija nalazi, dok se bezbednost RS/RM/IKTS odnosi na zaštitu CIA informacija koje se skladište, obrađuju ili prenose u RS/RM [61].

Bezbednost informacija omogućava kontinuitet poslovanja, smanjuje potencijalnu štetu, obezbeđuje povratak investicije i unapređuje ukupno poslovanje. U tom smislu se bezbednost informacija može definisati kao *odsustvo rizika za CIA informacija* ili *zaštićenost informacija od neovlašćenog pristupa, upotrebe, otkrivanja, izmene ili uništenja informacija* [6].

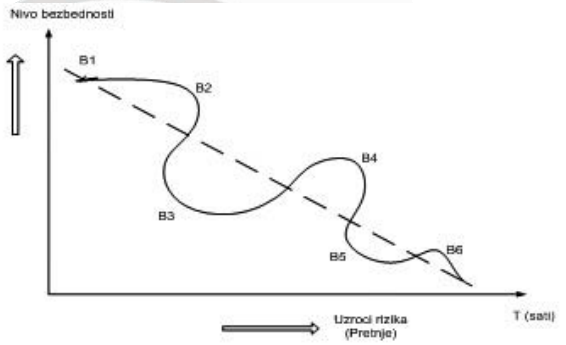
U praksi se bezbednost informacija najčešće manifestuje u bezbednom radu bez otkaza RS, RM i Interneta, malicioznih programa i prisluškivanja; bezbednoj komunikaciji, kupovini i plaćanju preko Interneta sa zaštitom privatnosti. Dakle, bezbednost informacija je ciklično ponovljiv *proces* stalnog održavanja zaštićenosti informacija, kojeg je potrebno *planirati, implementirati, izvršavati, održavati i poboljšavati,* kroz uspostavljen sistem za upravljanja zaštitom informacija – ISMS (*Information Security Management System*) [50].

2 Engl.: *Cyberspace Information Security.*

1.2.2. Funkcionalna zavisnost bezbednost – pretnje

Bezbednost IKTS je stanje i konkretno - situacioni problem realnog okruženja, pa ne postoji univerzalno i nepromenljivo stanje bezbednosti IKTS. *Agenti* potencijalnih pretnji su izvršioci *napada* i uzroci nastanka faktora rizika. *Rizik* je procenjena mera uticaja pretnje na informacionu imovinu i osnovna kategorija analize bezbednosti IKTS, a može se definisati kao *verovatnoća da će agent pretnje iskoristiti neku ranjivost sistema i izazvati negativne posledice za sistem i organizaciju u celini*. Kako apsolutna bezbednosti praktično ne postoji[3], upravljanje bezbednosti IKTS najbolje se objašnjava procesom *upravljanja rizikom*. U realnim uslovima, sa porastom pretnji povećavaju se rizici, a nivo ukupne bezbednosti IKTS nelinearno opada, zbog stepena neodređenosti uticaja faktora rizika (Sl. 1.2) [61].

Neka su B1, B2, ..., Bj, ...Bn bezbednosna stanja komponenti bezbednosti IKTS, procenjivana u prostoru i vremenu. Funkcija nelinearne zavisnosti komponenti bezbednosti – Bj od sto-hastički promenljivih faktora rizika – **Ri**, može se približno izraziti relacijom:



Sl. 1.2. Nivo ukupne bezbednosti IKTS u funkciji pretnji

$$B_j = \sum_{j=1}^{n} k_j B_j \left(1/R_i\right)$$

gde su: *j=1,2,...,n* – komponente bezbednosti,
k=1,2,…,*n* – težinski faktori *uticaja* pojedinačnih komponenti bezbednosti, a
R_i – procenjeni faktori rizika pojedinačnih komponenti bezbednosti,
i=1,2,...,n.

Definisanje bezbednosnog stanja IKTS, sa formalnim matematičkim aparatom, nije lak zadatak, jer zahteva formalni opis IKTS i sistema zaštite. Relacioni pristup sa međusobnim odnosima relativno nezavisnih skupova ukazuje na težinu ovog problema. Neka je ukupna bezbednost IKTS predstavljena *skupom mogućih bezbednosnih stanja svih komponenti sistema zaštite* – **S,** u kojem *bezbednosna stanja pojedinačnih bezbednosnih komponenti IKTS* – $\mathbf{s}_i$ zavise od vrste, intenziteta i verovatnoće napada i uticaja iskoristivosti ranjivosti sistema sa kombinovanim, dinamički promenljivim pretnjama, na IKTS i poslovanje. Ako se uzme da okruženje IKTS unosi faktor *neodređenosti* u metriku

3 ako nisu na raspolaganju **neograničeni resursi** za zaštitu, što je praktično neizvodljivo.

nivoa bezbednosti IKTS i da je *trenutno bezbednosno stanje okruženja sistema (Bso)* = ***v***, elemenat *skupa svih mogućih stanja Bso* = **V**, tada se **V** može se definisati kao funkcija tri varijable [21]:

$$V = f(S, A, F)$$

gde je:

- **S** – skup mogućih bezbednosnih stanja svih komponenti bezbednosti sistema – $s_{i,}$ u kojem je identifikovan i definisan rizik i implementiran neki skup *upravljačkih, operativnih i tehničkih kontrola zaštite* koje smanjuju faktore rizika na prihvatljiv nivo;
- **A** – skup svih raspoloživih i novih *proceduralnih* kontrola zaštite – a_i, koje pomeraju sistem iz jednog u drugo (više) bezbednosno stanje;
- **F** – skup svih *tehničkih kontrola* komponenti sistema zaštite – f_i, koje su implementirane u specifičnim komponentama zaštite IKTS – s_i, na tekućem nivou bezbednosnog stanja sa faktorom rizika na prihvatljivom nivou.

Zadatak specijaliste zaštite je da definiše parove ($f_{i,}$ V_j), koji čine bezbednosno stanje komponente zaštite IKTS (s_i), prihvatljivim za organizaciju, što se može izraziti relacijom:

$$s_i\{f_i, V_j\}, \ \ j = 1, 2, \ldots, n$$

1.2.3. Glavni faktori uticaja na bezbednosno stanje IKTS

Na bezbednost IKTS utiču brojni, manje očigledni faktori, od kojih su najznačajniji funkcionalni zahtevi poslovnih sistema (npr. e-poslovanje, cloud computing-CC), organizaciona struktura (npr. promena prava pristupa, zbog promene posla), tehnološki razvoj (npr. problem zaštite u CC okruženju), politika zaštite (npr. nedostatak upravljačkog okvira na bazi politike za rešavanje tekućih problema zaštite), svest o potrebi zaštite (npr. implementacija tehnologije zaštite bez procene rizika), kompleksnost i skalabilnost sistema (npr. kompleksnost IKTS otežava postizanje koherentnog sistema zaštite), poverljivost i privatnost (npr. kompleksan problem prenosa poverenja u IKT okruženje) i dr. [74, 85, 35, 59, 63].

K*valitetne i integrisane informacije*, potrebne za odlučivanje, postaju najznačajniji resurs svake organizacije i kritični objekat zaštite. Izvršni menadžeri rangiraju zaštitu informacija sa 7,5 od 10, po značaju za funkcionisanje IKTS [28]. Na *kvalitet informacija* utiče niz atributa (*tačnost, blagovremenost, aktuelnost, pouzdanost, integritet, objektivnost, tajnost, raspoloživost* i dr.), koji pojedinačno mogu biti od relativnog značaja za različite poslovne sisteme. Sa porastom informatizacije svih sfera života raste značaj *kvalitetnih informacija*, koje u objektno orijentisanom pristupu obezbeđuje bezbedan IKTS. Zato se ukupan kvalitet poslovnih IKTS često ilustruje *trouglom stabilnosti: hardver, softver, bezbednost.*

Činjenica da je vrednost informacija funkcija vremena (informacija značajna danas ne mora biti značajna i sutra), presudno utiče na način zaštite informacija. Na primer: informacije, koje obezbeđuju komparativnu prednost za duži vremenski period, treba štititi jakim mehanizmima zaštite (npr. kriptološkim). Otuda i potreba za razvoj realnih metoda za procenu rizika, kompatibilnih sa vremenskim okvirima i dinamikom savremenog e-poslovanja.

Zbog čestih *organizacionih* promena, pod uticajem brojnih ekonomskih i tehnoloških faktora, osnovni problem je kako obezbediti specijaliste zaštite sa potrebnim znanjima i veštinama i izvršne menadžere, koji najbolje poznaju poslovne procese, identifikuju faktore rizika, određuju prava pristupa, upravljaju sistemom zaštite itd.

Tehnološki razvoj pomera težište sa automatizacije poslovanja na *integraciju sistema* i *integrisano upravljanje* kompleksnim upravljačkim i inženjerskim procesima, što otežava administraciju zaštite IKTS, koju je vrlo teško ili nemoguće potpuno automatizovati i integrisati. Zato intervencija čoveka u sistemu bezbednosti informacija, ostaje nezamenljiv i kritičan faktor.

Kompleksnost savremenih, heterogenih, visoko distribuiranih IKTS, glavni je problem za planiranje arhitekture sistema zaštite, zbog teškoća identifikovanja i korekcije ranjivosti. Razvojem *veb* servisa i aplikacija[4], IKT i Internet umrežavanja, generisani su sasvim novi tipovi pretnji, koje zahtevaju razvoj novih *modela, procesa* i *kontrola* zaštite.

U većini organizacija procesi zaštite su nedovoljno razvijeni i stabilni i aksiomatski zavise od predefinisane *politike zaštite* i procene izloženosti faktorima rizika na bazi statičkog okvira ISMS standarda[5] za upravljanje zaštitom, operativnih uputstava i tehničkih kontrola zaštite. Relevantni standardi zaštite identifikuju sva ograničenja sistema zaštite, projektovanog na bazi predefinisane *politike zaštite* i sugeriše regularnu *procenu rizika* [48, 49, 50, 84]. Ovaj pristup podrazumeva da se procena rizika uzima kao primarni alat za donošenje odluka, što ne znači da upravljački okvir na bazi politike zaštite nije važan. Naprotiv, treba ga redovno koristiti, ali samo češće kontrolisati njegovu relevantnost u realnom kontekstu i na bazi procene rizika.

Veći problem je nedostatak svesti menadžera o potrebi procene rizika, koji češće implementiraju tehnologije zaštite bez procene rizika, kao i krajnjih korisnika koji nedovoljno shvataju potrebu kontrole i posledice uticaja rizika na dnevne aktivnosti. Forsiranje primene tehničkih rešenja zaštite, može stvoriti iluzija da se rizik uspešno kontroliše i da bezbednost zavisi od primene sve novijih i novijih alata. Iako u zaštiti IKTS dominiraju tehnološka pitanja, treba izbegavati projektovanje arhitekture sistema zaštite samo na bazi tehnologije i standarda najbolje prakse zaštite. Racionalan pristup obezbeđuje samo razumevanje *realnog rizika* i njegovog relativnog značaja za organizaciju.

Na praksu zaštite IKTS, glavni uticaj imaju: *kompleksnost, skalabilnost, poverljivost i privatnost*. *Kompleksnost* zahteva duboko razumevanje principa funkcionisanja IKTS, da bi se implementirao koherentan sistem zaštite. *Zahtev za skalabilnost* (nadogradi-

4 SOA, mrežno računarstvo (*Greed Computing*), distribuirano Internet računarstvo (*Cloud Computing*)

5 Standard ISO/IEC 27001

vost) raste uporedo sa porastom kompleksnosti, distribuiranosti i umrežavanja IKTS, što automatski zahteva analizu modularnosti i mogućnosti integracije. *Poverljivost i privatnost* su dva ključna pitanja koja dramatično rastu sa povećavanjem broja umreženih aplikacija i primene IKTS, servisa i aplikacija. Modeli autentifikacije (verifikacije identiteta) postali su tehnički najkompleksnija oblast zaštite savremenih IKTS u Internet okruženju, pošto su jedini mehanizmi koji mogu rešiti istovremeno probleme uzajamnog poverenja i zaštite privatnosti korisnika. Zahtevi za zaštitom privatnosti i poverljivosti ličnih podataka rastu uporedo sa lakoćom sa kojom se elektronske informacije mogu skladištiti, prenositi, menjati i distribuirati. U većini zemalja u svetu doneti su zakoni za zaštitu privatnosti ličnih podataka u elektronskom okruženju, dok se pristup ovom problemu bitno razlikuje od zemlje do zemlje [75, 76, 77]. U sekciji *Osam izveštaja privremenog komiteta evropskog parlamenta* navodi se da: „*Svaki akt koji uključuje intercepciju komunikacija i čak snimanje podataka od strane obaveštajnih službi za obaveštajne namene, predstavlja ozbiljno kršenje lične privatnosti*". Međutim, porast terorizma u svetu i kompjuterskog kriminala nameću potrebu da se izbalansiraju prava zaštite privatnosti i potrebe država da imaju pristup svim informacijama i podacima.

Generalno, bezbednost realnog IKTS zavisi od sledeća četiri faktora: šta sistem treba da radi (specifikacija/politika), kako to radi (implementacija/mehanizmi zaštite), da li stvarno to radi (tačnost/garantovana bezbednost) i može li sistem preživeti sofosticirane napadače (ljudska priroda)[6].

Na primer, krajem 2010. godine dnevno se na Internetu generisalo oko 40.000 novih, sofisticiranih tipova pretnji, od koji preko 40% promeni svoju definiciju u prva 24 časa[7]. Održavanje stanja bezbednosti IKTS, u nebezbednom okruženju, treba da bude stabilan proces. U praksi to se stanje bezbednosti održava na prihvatljivom nivou rizika sa implementiranim upravljačkim (**U**), organizacionim (**O**) i tehničkim (**T**) kontrolama zaštite [100].

1.3. OPŠTA DEFINICIJA SISTEMA ZAŠTITE

Zahtevana bezbednost informacija i IKTS ostvaruje se (pod)sistemom zaštite. U objektno - orijentisanom pristupu, sistem zaštite je *organizovan i koherentan skup* **U, O** *i* **T** *kontrola zaštite i njihovih veza i ograničenja, primenjenih na IKTS, da bi se zaštitila raspoloživost, poverljivost i integritet (uključujući neporecivost i autentifikaciju), procesiranih, uskladištenih i prenošenih podataka i informacija i održao ili povećao nivo bezbednosti i pouzdanosti funkcionisanja IKTS u izvršavanju poslovnih ciljeva i misije organizacije*. Ova definicija nedvosmisleno implicira da sistem zaštite IKTS nije sam sebi cilj, nego da je u funkciji pouzdanog funkcionisanja IKTS u izvršavanju poslovnih ciljeva i misije organizacije.

6 Stamp, M., *Information Security: Principles and Practice,* JohnWiley & Sons, Inc. 2006.

7 *The Help Net Security News*, 17. novembar 2010.

Za analizu i razvoj *sistema zaštite* najbolje rezultate daju metodologija sistem inženjerske analize, objektno - orijentisano modelovanje (OOM) i procesni pristup, čija je glavna prednost smanjivanje kompleksnosti [21]. Prva faza razvoja sistema zaštite je definisanje modela IKTS i određivanje objekata koje treba štititi, na bazi procene rizika. Racionalno je razvijati sistem zaštite za životni ciklus IKTS.

U pristupu zaštiti informacija, glavni cilj je fokusirati pažnju na procenu rizika i izbor kontrola zaštite za ublažavanje tog rizika na prihvatljiv nivo. Kako je *profil rizika* specifičan za svaku organizaciju, primena *standarda najbolje prakse zaštite*[8] nije uvek adekvatna, pošto ne uzimaju u obzir različite profile rizika. Drugim rečima, *optimalni sistem* zaštite informacija ne znači obavezno najviši nivo zaštite, kojeg podrazumeva *standard najbolje prakse zaštite*, nego – rentabilan, ekonomski i funkcionalno opravdan sistem zaštite za dato poslovno okruženje, profil rizika i ukupne troškove zaštite. Kako je IKTS bezbedan, ako je adekvatno zaštićen, bezbednost IKTS – B_{IS} je *bezbednosna funkcija* sistema zaštite – Sz, tj:

$$B_{IS} = f(S_z)$$

Bezbednost IKTS se dovoljno dobro može definisati i skupom atributa *vektora zaštite*, gde je: *intenzitet zaštite* (dužina vektora)–**Isz,** *kvalitet zaštite* (pravac vektora) – **Ksz** i *sveobuhvatnost (višeslojnost* i *raznovrsnost) kontrola zaštite* (smer vektora zaštite) – **Ssz**, pa je:

$$B_{IS} = f(S_z) = f(I_{sz} \mathbf{U} K_{sz} \mathbf{U} S_{sz})$$

Atributi vektora zaštite su u konjuktivnoj vezi, pa sledi da će IKTS biti bolje zaštićen, ako je veća unija atributa, odnosno što je sistem zaštite koherentniji.

1.3.1. Osnovne funkcionalnosti sistema zaštite

Osnovne funkcionalnosti sistema zaštite izvršavaju se kroz *servise, mehanizme, kontrole* i *funkcije zaštite* ili *bezbednosne funkcije*. Funkcije zaštite se izvršavaju *mehanizmima* i *protokolima* zaštite, koji u logičkom smislu predstavljaju način realizacije *servisa zaštite* [63, 74, 83].

Servisi zaštite su logičke aplikacione jedinice, koje se izvršavaju kroz različite akcije, kao što su *metodi za implementaciju operacija kontrola zaštite*, *funkcionisanje ili transformisanje bezbednosnih funkcija*, *implementacija skupa politika zaštite, rukovanje mehanizmima zaštite, ažuriranje, dodavanje, modifikacija sa novim rešenjima zaštite itd.* Servis zaštite je proces ili neprekidna, ponovljiva aktivnost, izvršena funkcijama mehanizama i protokola zaštite. Korisnike ne zanima kako su servisi zaštite implementirani, već da li mogu da izvrše željenu akciju. Na primer: *zaštita tajnosti informacija* u komunikacionom kanalu je servis zaštite u IKTS, a algoritamska *kriptografska transformacija* sadržaja informacija je mehanizam za realizaciju tog servisa zaštite.

8 NIST SP 53 A, B, C; ISF v.4.0; ISO/IEC 27000 serija, ISO/IEC 21827 (SSE CMM) itd.

Mehanizmi i protokoli zaštite su individualni algoritmi, hardversko-softverski moduli ili metodi za izvršavanje bezbednosnih funkcija. Neki mehanizmi zaštite su za jedan, a neki za više različitih servisa (npr. *kriptografski* mehanizmi). Za realizaciju mehanizma zaštite, potrebno je obezbediti određene *kontrolne strukture*, koje mogu biti *upravljačke, operativne i tehničke,* a uobičajeno se nazivaju *kontrole zaštite*.

Kontrola zaštite IKTS je konačna klasifikacija mehanizama zaštite i interfejs između mehanizma i čoveka. *Kontrola zaštite* može biti *tehnička* povratna sprega (npr. alarmni signal generisan na izlazu IDPS), bezbednosna funkcija arhitekture sistema zaštite, *organizaciono-operativna mera* (npr. barijere za fizički pristup) i *upravljačko–administrativna mera* (npr. primenjen standard). Termin *kontrola zaštite*, takođe, implicira suštinsku potrebu neprekidnog nadzora i *kontrolisanja* sistema zaštite i uspešno zamenjuje tradicionalne termine: *administrativnih, organizacionih i hardversko softverskih mera i metoda zaštite* [33].

1.3.2. Informacioni sistem kao objekat zaštite

Osnovno *strukturno obeležje* savremenih IKTS je teritorijalna distribucija RM u intenzivnoj komunikaciji sa RS, kao osnovnom tehničkom komponentom. S*manjenje kompleksnosti* postiže se uvođenjem *grana objekata* [21, 61]:

- **informacione imovine:** *poverljivost (**C**), integritet (**I**) i raspoloživost (**A**) ili **CIA**[9],* čime se struktuiraju objekti koje treba štititi, tj. bezbednosni ciljevi i
- **mera i sredstava zaštite**: *proceduralne* (U, O) i *tehničke* (T) *kontrole* zaštite, čime se struktuiraju alati za zaštitu.

U objektno orijentisanom pristupu zaštita informacija podrazumeva zaštitu *informacione imovine*: *čiste, fizičke* i *humane* (tabela T.1.1) [50, 51].

Tabela 1.1 Klasifikacija informacione imovine

Čista informaciona imovina	
Digitalni podaci i informacije	personalne, finansijske, zakonske, istraživanje i razvoj, strateške i komercijalne, e-pošte, *voice*-mail, baze podataka, lični i deljeni folder, *backup* mediji – trake/CD/DVD i digitalna arhiva, šifarski ključevi, lozinke
Opipljiva informaciona imovina	personalna, finansijska, zakonska, istraživanje i razvoj, strateške i komercijalne, poštanske pošiljke, faksovi, mikrofiš i drugi bekap/arhivni materijali, ključevi skladišta medija, žurnala, magacina, knjiga
Neopipljiva inf. imovina	znanje, poslovni odnosi, trgovačke tajne, licence, patenti, iskustva, brend, reputacija, poverenje, konkurentnost, etika, produktivnost
Aplikativni program	razvijeni u korporaciji/kastomizovani sistemi, klijentski program (uključujući deljene i za krajnje korisnike), komercijalno raspoloživi softver, ERP sistemi, MIS (*managament IS*), baze podataka, uslužni programi/alati, aplikacije za e-poslovanje, *midleware*
Sistemski program	za servere, desktop računare, *mainframe* računare, mrežne uređaje, priručne i ugrađene računare (uključujući bios rom i druge *firmware*

(nastavak na sledećoj strani)

9 Engl.: CIA – *Confidentiality*, *Integrity and Availability* (poverljivost, integritet i raspoloživost)

Fizička informaciona imovina	
Infrastruktura za podršku IKTS	zgrada u kojoj su smešteni: IKTS, centar za obradu podataka, serverske/računarske sobe, kancelarije, kabina za umrežavanje LAN mreže, kabineti za držanje fascikli dokumenata, sobe i sefovi za čuvanje EM i optičkih diskova, uređaji za identifikaciju i autentifikaciju medija/ kontrolu pristupa (kartični sistemi za pristup, tokeni, smart kartice itd.) i drugi uređaji za tehničku zaštitu (CCTV, protivprovalni sistemi itd.)
Kontrole okruženja IKTS	protivpožarni alarmi/sistemi za gašenje požara/protivpožarni aparati, jedinice za neprekidno napajanje (UPSS), mrežno napajanje, mrežni transformatori/filteri/atenuatori, klima uređaji/ventilacioni sistemi za provetravanje, alarmni sistemi za poplavu
Hardver IKTS	uređaji za računanje i skladištenje (desktop PC, radne stanice, laptop, priručni računari, serveri, *mainframes*, modemi i linijski terminatori, komunikacioni uređaji, (mrežni čvorovi), printeri/kopir/fax mašine itd.
Imovina IKTS	autentifikacioni servisi i administrativni procesi za upravljanje profilom korisnika, hiperlinkovi (brauzeri), *firewalls*, *proxy* serveri, mrežni servisi, bežični servisi, anti–spam/ virus/*spyware*, IDPS, servisi za telerad, servisi zaštite, FTP, e–mail, web servisi, ugovori za podršku i održavanje.
Humana informaciona imovina	
Zaposleni	zaposleno osoblje, glavni/izvršni menadžeri, dizajneri/programeri/ evaluatori programa, menadžer i administrator zaštite, operateri, pravnici, korisnici sa najvećim privilegijama, LAN i administratori zaštite.
Ne-zaposleni	privremeno zaposleni, spoljni konsultanti/specijalisti savetnici, specijalisti po ugovoru, snabdevači, poslovni partneri

Osnovni bezbednosni zahtevi za sistem zaštite informacija su sprečavanje: *ugrožavanja bezbednosti ličnosti, organizacija i države; krađe, pronevere, gubitaka i izmene informacija; neovlašćenih aktivnosti u IKTS; povreda intelektualne svojine, privatnosti i poverljivosti ličnih i poslovnih podataka u skladu sa Zakonom o zaštiti podataka o ličnosti* [10] i *Zakonom o zaštiti tajnosti podataka*.

Sistem zaštite informacija je *podsistem* IKTS i postaje najvažnija komponenta razvoja savremenih IKTS, svih tipova i namena; integriše se u IKTS kroz opšte funkcionalne komponente sistema ili dodatne komponente i posebne kanale, koji spajaju elemente jednog sistema sa drugim. Normalno, IKTS se uglavnom zasnivaju na standardnim hardversko–softverskim proizvodima. Mehanizmi i protokoli zaštite, koji za svoj rad koriste funkcije IKTS, u velikoj meri zasnivaju se na tehničkoj pouzdanosti IKTS. Standardi zaštite preporučuju da se sistem zaštite projektuje paralelno i u toku razvoja prve faze životnog ciklusa, a implementira u fazi implementacije samog IKTS, za sve faze životnog ciklusa IKTS.

U procesima definisanja bezbednosnih ciljeva, planiranja i projektovanja sistema zaštite, u prvom koraku treba razmatrati bezbednosno relevantne komponente IKTS: *mrežnu arhitekturu, topologiju, infrastrukturu*, *protokole*, *servise*, *platforme* i *aplikativne programe* (Tabela 1.2) [21].

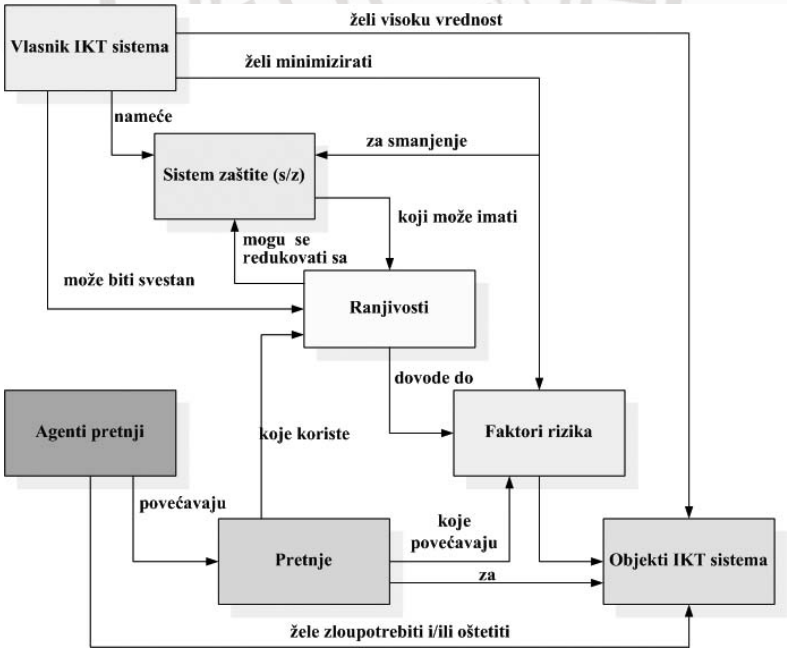
10 U Republici Srbiji stupio na snagu 01.01.2009.

Tabela 1.2. Relevantni aspekti zaštite IKTS

Aspekti zaštite	Objekti zaštite za analizu
Ključne karakteristike IKTS	vrsta komunikacionih veza i uređaja i procesi upravljanja, kompleksnost formalnog opisa IKTS, raznorodnost i prostorna distribucija komponenti IKTS, vrste prezentacije servisa, upravljanje procesima i umrežavanje
Servisi IKTS	uspostavljanje veze, predaja podataka, obrada podataka udaljenim pristupom, prenos datoteka, e-pošta, pristup distribuiranim bazama i dr.
Kvalitet IKTS servisa	*ukupan broj veza* – potencijalna sposobnost uspostavljanja međusobnih veza korisnika i distribuiranih objekata sistema
	vremenska karakteristika – brzina isporuke servisa korisnicima na bazi srednjeg vremena pristupa (zavisi od veličine, udaljenosti i opterećenja)
	srednje vreme isporuke servisa – vreme utrošeno na obradu zahteva korisnika u nekom režimu rada sistema
	pouzdanost servisa – verovatnoća rada sistema bez otkaza
	vernost prenosa, pohranjivanja i integriteta informacija, određena brojem sistemskih grešaka i pristupnih tačaka informacijama i podacima

1.3.3. Generički, funkcionalni model sistema zaštite

Za razumevanje mesta i uloge sistema zaštite IKTS, od velike koristi je *generički model sistema zaštite* (Sl. 1.3).



Sl. 1.3. Generički model sistema zaštite i međusobni odnosi komponenti

Vlasnik IKTS uspostavlja vrednosti informacione imovine i odgovoran je za njenu zaštitu. *Agent pretnje* je izvršilac potencijalne pretnje i uvek radi protiv interesa vlasnika sistema. *Sistem zaštite* štiti objekte informacione imovine od *pretnji* – tipično malicioznih programa i namernih internih i eksternih napada, koje ugrožavaju *poverljivost, integritet i raspoloživost* objekata informacione imovine. Vlasnik, u *proceni rizika*, analizira moguće pretnje i procenjuje, koja od njih je primenljiva u okruženju; procenjuje ranjivosti sistema, iskoristivost te ranjivosti sa jednom ili više pretnji i verovatnoću uticaja na poslovanje. Rezultati analize su rizici. Analiza i procena rizika uključuje izbor različitih *kontrola zaštite* za ublažavanje rizika na prihvatljiv nivo, smanjenjem *ranjivosti* i *izloženosti* u skladu sa zahtevima *politike zaštite* vlasnika. Posle implementacije kontrola zaštite, agenti pretnji mogu iskoristiti preostale ranjivosti, što predstavlja *preostali rizik na prihvatljivom nivou*, kojeg vlasnik u neprekidnom (cikličnom) procesu zaštite uvek nastoji smanjiti svim raspoloživim kontrolama zaštite. Vlasnik mora biti uveren da su primenjene kontrole zaštite adekvatne za ublažavanje faktora rizika, pre nego što dozvoli izlaganje IKTS – identifikovanim pretnjama. U tom cilju, vlasnik može tražiti *evaluaciju* – internu i spoljnu reviziju (*audit*) ili *sertifikaciju* i *akreditaciju* (testiranje i odobrenje za rad) IKTS i sistema zaštite. Izlaz procesa evaluacije je izjava o *akreditatciji* (na bazi rezultata *sertifikacije*) da će zaštitne mere smanjiti faktore rizika na prihvatljiv nivo. Na osnovu rezultata evaluacije vlasnik odlučuje da li će prihvatiti preostali rizik ili ne, što dokazuje potpisivanjem dokumenta SOA (*Statement of Applicability*) [12, 51].

1.3.4. Definisanje optimalnog sistema zaštite

Namena *programa zaštite* informacija je da identifikuje bezbednosne ciljeve i razvije, implementira i održava *optimalan* (ekonomski rentabilan i funkcionalno efektivan) sistem zaštite. Neki IKTS je *optimalno zaštićen,* ako ima izbalansirane *efektivnosti* kontrola zaštite i *troškove* njihove akvizicije/razvoja, odnosno, kada su troškovi kontrola zaštite potpuno izjednačeni sa procenjenim gubicima [4].

U zavisnosti od odnosa strategije zaštite i postavljenih bezbednosnih ciljeva, moguća su dva pristupa sintezi *optimalnog sistema zaštite* [21]:

Primarni: za dati nivo troškova zaštite – **Trz** obezbediti maksimalno mogući intenzitet vektora zaštite – **I (s) =>I_{max}**, gde je **s** – izabrana strategija zaštite;

Sekundarni: obezbediti željene rezultate intenziteta vektora zaštite **I(s) > $I_{dopušteni}$,** pri minimalno mogućim troškovima zaštite **– T_{trmin}**

Pod *efektivnošću kontrole zaštite* informacija podrazumeva se efikasnost i efektivnost u aktivnoj zaštiti poverljivosti, integriteta i raspoloživosti informacija u operacijama obrade, skladištenja i prenosa. Ocena efektivnosti procesa zaštite odnosi se na sposobnost kontrole zaštite da reši zadatak zaštite.

U procesu sinteze optimalnog sistema zaštite, početne aktivnosti su izbor matematički produktivnog kriterijuma optimalnosti, u skladu sa arhitekturom sistema zaštite, tehnologijom obrade informacija i preciznom matematičkom formulacijom zadatka, uzimajući u obzir sve apriorne zaključke i dopuštena rešenja u skladu sa primarnim kriterijumima. Za sintezu optimalnog sistema zaštite treba imati gotova rešenja za *arhitekturu sistema zaštite i ocenu kvaliteta njenog funkcionisanja, ocenu osetljivosti modela razvoja u odnosu na apriorne podatke i fizičku realizaciju integrisanog sistema zaštite u IKTS*.

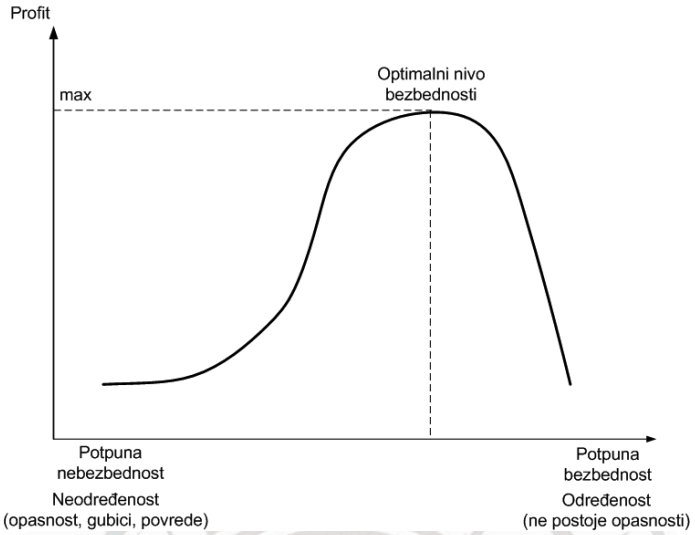
Izbor vektora *efektivnosti kontrole zaštite* – **I(s)** zavisi i od izbora *strategije zaštite* – **s**, koja se određuje iz skupa strategija zaštite – **S**. U opštem slučaju ta zavisnost se izražava relacijom transformacije–**Y** skupa mogućih strategija – **S** u skup *indikatora efektivnosti* – **I** [21]:

$$Y : S \rightarrow I$$

Uvođenje indikatora efektivnosti – **I** zahteva takvo određivanje kriterijuma efektivnosti, koji omogućavaju izbor strategije iz skupa dostupnih. Pri tome, neophodno je uzeti u obzir da teoretske osnove za formiranje optimalnih sistema zaštite nisu dovoljno usavršene. Za sintezu optimalnih sistema, osim nedostatka dovoljno tačne opšte teorije za formiranje *metodoloških osnova* za fenomene sa faktorima neodređenosti, nije primenljiva ni klasična statistička teorija.

Pod *metodologijom optimizacije* sistema zaštite informacija podrazumeva se razvijena teorija zaštite, koja povezuje strukturu sistema zaštite, logičku organizaciju i kontrole zaštite u cilju formiranja bezbednosnih funkcija za izbor i izdvajanje podskupa najboljih strategija zaštite. *Optimalno rešenje zaštite je ono, koje u datim uslovima na najbolji način zadovoljava sve uslove razmatranog zadatka, a postiže se putem najracionalnije raspodele resursa utrošenih na rešavanje zadataka zaštite* [21]. U procesu uspostavljanja optimalnog sistema zaštite potrebno je vršiti korekciju zahteva, zbog faktora neodređenosti *ponašanja, funkcionalnosti ili ciljeva zaštite*. Osnovni nedostaci optimizacije sistema zaštite odnose se na *matematičku složenost rešavanja optimalnog sistema, težinu programiranja algoritma optimizacije, neprihvatljivo veliko vreme automatske optimizacije i zavisnost kvaliteta optimalnog sistema od tačnosti izvornih ovlašćenja i karaktera promena upravljanog objekta zaštite*.

Generalno, optimalni sistem zaštite dobije se u tački između potpune bezbednosti i ne–bezbednosti, uz ostvarivanje maksimalnog profita (Sl. 1.4) [4].



Sl. 1.4. Optimalni sistem zaštite informacija

Sa porastom troškova akvizicije/razvoja sistema zaštite, raste i nivo bezbednosti IKTS, ali opada potencijalni profit organizacije zbog troškova sistema zaštite. Zato ne treba težiti sve većem i većem nivou zaštite po svaku cenu.

1.3.5. Promena paradigme zaštite IKTS i informacija

U zaštiti IKTS bazična su dva principa:

- *po dubini*, implementacija serije nezavisnih mehanizama zaštite za sprečavanje kompromitacije sistema, probojem nekog sloj i
- *primarna zaštita najvrednije imovine*, alokacija resursa organizacije za zaštitu najvrednije informacione imovine – informacija.

Ova dva principa su tradicionalno grafički prikazivana sa *prstenovima zaštite* ili tzv. *slojevima luka*, koji višekratno preklapaju *jezgro*. Savremeni razvoj SOA[11] web aplikacija, virtuelizacija klijentske i serverske strane i razvoj distribuiranog Internet računarstva – **CC** (*Cloud Computing*), kao i neki drugi faktori, zahtevaju promenu klasične paradigme zaštite, bazirane na ova dva principa.

Savremene organizacije sve više diverzifikuju lanac vrednosti, u kojem učestvuju različite organizacije, koje igraju jednako značajne uloge. Sa aspekta zaštite IKTS, to znači da će neki slojevi zaštite biti efektivni, samo ako se implementiraju u svim organizacijama koje učestvuju u distribuiranom lancu vrednosti.

11 Engl.: SOA (*Service Oriented Application*) – servisno orijentisane web aplikacije.

Ekonomske i finansijske krize su uzrok velikog broja nezaposlenih i čestih promena posla širom sveta, pa nezadovoljni, vešti profesionalci sa administrativnim privilegijama i slabim etičkim principima, mogu predstavljati ozbiljne pretnje za savremene IKTS (npr. izbrisati, modifikovati ili prodati–vredne podatke). Gubitak granica organizacije i postojanje ozbiljnih internih pretnji, menjaju paradigmu zaštite od *slojeva luka* na *prsten slojeva luka* ili distribuiranu slojevitu zaštitu po dubini. U ovim uslovima organizacije moraju implementirati takav sistem zaštite, koji je otporan na interne pretnje i obezbeđuje poslovanje, čak i kada je probijen.

Virtualizacija klijentske i serverske strane smanjuje vreme i resurse, potrebne za uvođenje novih sistema u organizaciju. Takođe, stariji sistemi mogu biti virtuelizovani. Sa aspekta bezbednosti, otvoreno je novo polje za istraživanje adekvatnih mehanizama zaštite hipervizora u konfiguraciji virtuelne mašinske introspekcije (VMR), koji bi sprečili nedozvoljenu komunikaciju između virtuelnih mašina (VM). Veoma brzo, zaštita informacija u virtuelnom okruženju **CC** postaće sve značajnija oblast za istraživanje i razvoj. Za iznajmljivanje softvera kao servisa (**SasS**), hardvera (**HasS**) ili infrastrukture (**IasS**), potrebno je samo da se klijent, preko Interneta, poveže sa poslovnom aplikacijom provajdera **CC** usluga. Rad u **CC** nudi brojne prednosti za organizaciju, ali nosi i nove probleme zaštite, kao što su[12]: kako zaštititi podatke organizacije u **CC** i koje servise za zaštitu CIA informacija treba da obezbede klijenti, a koje provajderi **CC** itd.

Evolucija mobilnih telefona, od prostog telefona sa nekim funkcionalnostima PDA (*Personal Digital Assistant*) do uređaja, koji je po funkcionalnosti bliži personalnom računaru, nego bazičnom telefonu. Razvoj mobilne telefonije je uneo dodatnu kompleksnost u oblast zaštite, jer zahteva slične mehanizme zaštite, kao za desktop, laptop i priručne računare (AVP, personalna barijera i ažuriranje softvera).

Upotreba digitalnih RS i RM za izvršavanje krivičnih dela, kao što su prevare, uznemiravanja, distribucija ilegalne pornografije i krađa intelektualne imovine i identiteta, postala je surova realnost. Kada se dogodi glavni kompjuterski incident, organizacija u prvom koraku pokušava utvrditi prirodu incidenta i veličinu štete, svojim kapacitetima za upravljanje kompjuterskim incidentom. Kad slučaj prevazilazi nadležnosti organizacije, incident se prijavljuje zvaničnim organima istrage. U oba slučaja počinje istraga kompjuterskog incidenta/kriminala, koja uključuje ispitivanje digitalnih dokaza. Profesionalci, specijalizovani za digitalnu forenzičku istragu su nezamenljivi u ovom poslu.

Kako se povećava broj digitalnih uređaja, sve više raste značaj dnevnika rada (*log* datoteka) svih tih uređaja, zbog potrebe praćenja bezbednosno relevantnih događaja. Za pregled i reviziju obimnih podataka u brojnim *log* datotekama, potrebni su neprihvatljivo veliki resursi. Zato je automatizovana analiza log datoteka na bezbednosno relevantne događaje, od velikog značaja za nadzor sistema zaštite savremenih IKTS. Sveobuhvatni pristup proveri i reviziji svih distribuiranih log datoteka nije moguć, pa je dobro rešenje centralizovano skupljanje svih log podataka u *log server*. *Aktivna, selektivna analiza bezbednosno-relevantnih događaja u log serveru, na bazi specifičnog poznavanja realnih pretnji, koje pogađaju kritične poslovne procese, postaje ključ za ranu detekciju incidenta*.

12 Grubor, G., Njeguš, A., *Paradigma zaštite distribuiranog računarstva*, Singergija 10, 2010.

U novom e-okruženju, organizacije moraju generičku metodologiju za upravljanje rizikom dopuniti sa agilnijim tehnikama, zasnovanim na činjenicama, dobijenim *mikoranalizom rizika,* umesto scenarija rizika na *makro* planu. To znači da upravljanje rizikom mora postati obavezan deo poslovnog odlučivanja, na bazi realnih, lokalnih i specifičnih pretnji, ranjivosti i uticaja na poslovne procese.

Digitalno okruženje postaje značajan front u savremenom ratovanju, a u budućnosti njegov značaj će još više porasti. Više armija u svetu (preko 120) dizajnira, implementira, testira i uvodi defanzivne i ofanzivne alate za scenario kiber ratovanja. Poznato je da se praktično vode kiber ratovi između Indije i Pakistana, Rusije i Gruzije, Izraela i Palestine, a Kina sama već je angažovala više od 10.000 specijalista za kiber ratovanje.[13]

Upravljanje rizikom na mikro nivou, obezbeđuje tehnike koje su primenljive i za detekciju malicioznih programa. U toku je razvoj novih alata kao što su šire dostupne *kriptografske tehnike i tehnologije višeslojne mrežne zaštite* (distribuirane barijere, sistemi za detekciju i sprečavanje upada – IDPS (*Intrusion Detection and Protection Systems),* distribuirani sistemi za monitoring i kontrolu saobraćaja (skeneri, *veb* filteri), sistemi za centralno upravljanje zaštitom preko zaštićenih veza, *proaktivni sistemi zaštite* od poznatih i nepoznatih pretnji, objektno orijentisani i procesni pristup za smanjenje kompleksnosti zaštite, *programi* koji obezbeđuju servise zaštite na heterogenim platformama itd. Za zaštitu korisničkih informacija u web i CC okruženju, nije dovoljno samo implementirati tradicionalne mehanizme zaštite, nego ih je potrebno ugrađivati u distribuirane hardverske uređaje i softver u fazi njihovog razvoja i proizvodnje.

Na nekoliko univerziteta u svetu, u toku su istraživanja kolonije tzv. *digitalnih mrava*, koji u svemu podražavaju prirodne mrave. Specifična grupa digitalnih *mrava* programira se za jednu vrstu malicioznog programa, na koji se nakon detekcije fokusiraju i alarmiraju administratora za nadzor sistema zaštite.

1.3.6. Opšti metod implementacije sistema zaštite

Glavni cilj svakog sistema zaštite je da obezbedi efikasno upravljanje rizikom. Odnosno, rizik nije moguće redukovati ako *sistem zaštite* nije implementiran i integrisan u IKTS za podršku poslovnih procesa. Odgovornost za to imaju svi zaposleni i menadžment organizacije, koji mora imenovati odgovarajuća lica za koordinaciju i nadgledanje procesa realizacije sistema zaštite. Ova lica moraju biti sposobna da identifikuju interne i eksterne faktore rizika za CIA podataka i informacija, uključujući i rizik od nedovoljne i nekvalitetne obuke u oblasti zaštite.

U praksi zaštite, između više raspoloživih, najčešće se primenjuju dva metoda za implementaciju sistema zaštite [68,69]:

1. *sveobuhvatno ublažavanje ukupnog rizika na prihvatljivi nivo i*
2. *proces 4–fazne tranzicije iz jednog u drugo bezbednosno stanje*.

13 EC, *Workshop on Information security,* INFRA 42589, Hotel Šumadija, Beograd, 4-5.10.2010

Smanjenje ukupnog rizika, za sve objekte IKTS, na prihvatljiv nivo, dugoročan je i zahtevan proces, koji podrazumeva sveobuhvatan, sistemski pristup i smanjenje svih faktora rizika, implementacijom adekvatnih i rentabilnih kontrola zaštite. Umesto istovremene zaštite svih objekta IKTS od svake iskoristive ranjivosti, preporučuje se alternativni metod 4–fazne tranzicije IKTS iz jednog u više bezbednosno stanje. Polazi se od zaštite najkritičnijih objekata IKTS. Pregled opštih faza implementacije sistema zaštite za ublažavanje faktora rizika, u zavisnosti od kritičnosti objekata koje ugrožavaju, dat je u tabeli 1.3 [69].

Tabela 1.3. Faze implementacije sistema zaštite

Faza	Kritični objekti za misiju	Kritični objekti	Primarni objekti	Opšti objekti
1.	20 glavnih faktora rizika–FR	0	0	0
2.	50 glavnih faktora rizika	20 glavnih FR	0	0
3.	100 glavnih faktora rizika	50 glavnih FR	20 glavnih FR	0
4.	200 glavnih faktora rizika	100 glavnih FR	50 glavnih FR	20 glavnih FR

U *1. fazi* štite se objekti *kritični za misiju* organizacije i ublažava 20 glavnih faktora rizika, ako procena rizika obuhvata ukupno 200 faktora rizika. Ovaj korak brzo daje rezultate i omogućava zaposlenim da prihvate proces proaktivne zaštite.

U *2. fazi* proširuje se sistem zaštite na sledećih 50 faktora rizika, kritična za poslove organizacije. Proces progresivno raste u skladu sa sazrevanjem kapaciteta zaštite organizacije, obezbeđujući sve dublje nivoe zaštite RM, RS i aplikacija.

Na ovom konceptu zasnivaju se metodi evaluacije ranjivosti, operativno kritičnih pretnji i informacione imovine – **OCTAVE** (*Operationally Critical, Threat, Asset, and Vulnerability Evaluation*) [68] i brze analize rizika – **BAR** [74]. OCTAVE omogućava da interni tim identifikuje faktore rizika za najkritičnije objekte IKTS i izgradi plan zaštite za ublažavanje tih faktora rizika. BAR analiza rizika se vrši na pojednostavljenoj arhitekturi IKTS, gde se objekti sa istim ili sličnim bezbednosnim ciljevima, grupišu u *bezbednosne zone*. U prvom koraku se ignorišu svi postojeći servisi zaštite, pošto ih proces BAR analize sam derivira. Skup rezultata BAR analize prikazuje se tabelarno u matrici faktora rizika, za svaku definisanu bezbednosnu zonu. BAR analizu rizika vrši tim izvršnih menadžera sa specijalistom zaštite, koji vodi sastanke i poznaje proces.

U svakoj metodi ublažavanja rizika osnovno pitanje je: kako prepoznati glavne faktore rizika? Za neke poslovne sisteme, moguće je za procenu ranjivosti sistema i primenu bezbednosnih popravki koristiti servis poverljivog provajdera zaštite – **TTPS** (*Trusted Third Party Service*) [11], koji prati pretnje na Internetu i dostavlja klijentima informacije o novim pretnjama ili aplicira bezbednosne popravke. Međutim, korišćenje usluga TTPS predstavlja značajan faktor nepoverenja korisnika i nije primenljivo za mnoge sisteme, zbog zakonskih i drugih ograničenja.

Proces implementacije sistema zaštite može se razlikovati u određenim aktivnostima, za različite ciljeve i okruženja organizacija. Generički *tok procesa implementacije sistema zaštite* odvija se u četiri faze [15]:

1. priprema (definisanje obima i granica projekta, izbor tima);
2. *identifikovanje bezbednosnih faktora rizika;*
3. *revizija* efikasnosti *kontrola* (sistema) *zaštite* i preporuke za izmene i
4. *integracija i prilagođavanje sistema zaštite* u skladu sa nalazima revizije.

Svaki proces implementacije sistema zaštite treba da obuhvata najmanje tri jasno diferencirane i obavezne komponente [1]: (1) *obuku zaposlenih*, (2) *nadzor kontrolu i reviziju usaglašenosti* i (3) *nametanje obaveze sprovođenja politike zaštite*.

Obuka zaposlenih uključuje detaljno upoznavanje svih zaposlenih sa politikom i procedurama zaštite koje se na njih odnose. Od zaposlenih se može očekivati odgovornost, samo ako su svesni šta se od njih očekuje. Bitno je shvatiti da je bezbednost kiber prostora više problem *ljudi* i *procesa*, nego *tehnologije*. Ljudski resurs je ključan za zaštitu informacija. Politika zaštite treba da eksplicitno i jasno istakne da će svaki zaposleni imati obuku za razvoj svesti i usavršavanje znanja i veština o zaštiti, na nivo, potreban za efikasno izvršavanje radnih obaveza.

Kontrola usaglašenosti meri stepen usaglašenosti, implementiranog i integrisanog sistema zaštite sa politikom, standardima i zakonima zaštite. Menadžment organizacije obezbeđuje i odgovaran je za *kontrolu opšte usaglašenosti* politike zaštite sa normativima i standardima i za implementaciju procesa koji nameću politiku zaštite. Monitoring zaposlenih je najlakši način da se nadgleda normativna usaglašenost politike i procedura, iako može biti u sukobu sa zakonom o zaštiti privatnosti zaposlenih. U većini organizacija u državnom i privatnom sektoru, ne očekuje se da zaposleni rade bilo šta privatno na računarima na poslu, pa u brojnim državama nisu zaštićeni zakonom o zaštiti privatnosti. U javnom sektoru u većini razvijenih zemalja zaposleni su zaštićeni *Zakonom o zaštiti ličnih podataka* i na računarima na poslu. Poslodavac je obavezan da upozori zaposlene da su svi podaci pod stalnim nadzorom. EU je obezbedila mnogo veću zaštitu privatnosti u privatnom i javnom sektoru, jer ima sveobuhvatan zakon o zaštiti privatnosti, koji se sve više globalno prihvata. Prema direktivi EU o zaštiti privatnosti mogu se monitorisati [20]: *pristup Internetu i filtriranje paketa, korišćenje e–pošte, saobraćaj brzih poruka, korišćenje telefona, lokacija zaposlenog (video nadzor) i logovanje otkucaja tastature.* U SAD zakon *Electronic Communication Privacy Act* iz 1996. godine štiti privatnost zaposlenih na radnom mestu (2001. godine oko 75% kompanija u SAD snimalo je i monitorisalo sav saobraćaj svojih zaposlenih). Prema tom zakonu, ako poslodavac upozori zaposlenog da se vrši nadzor, sud to priznaje kao pristanak zaposlenog. U Republici Srbiji od 1. januara 2009. godine na snazi je *Zakon o zaštiti informacija o ličnosti,* koji obuhvata i zaštitu poverljivosti i privatnosti ličnih podataka.

Kontrola specifične usaglašenosti prakse zaštite sa primenjenim standardima, politikom, procedurama i planom zaštite, zahteva verifikaciju *poslovnih procesa i operativnog korišćenja*

tehnologija zaštite. Za usaglašenost politike i prakse zaštite odgovorni su zaposleni izvršioci procesa, ako su za to na vreme obučeni, a usvojena znanja i veštine provereni. Sve više se koriste elektronski, interaktivni oblici politike zaštite, gde se korisnicima pre pristupa RS/RM na ekranu pojavi prozor, koji zahteva afirmativno prihvatanje saopštenja politike zaštite[14]. Ovakav program obuke je pogodan za najznačajnije faktore rizika (npr. *korišćenje Interneta, e-pošte i pristup zaštićenim podacima*), ali ne i za celu politiku zaštite. Preporučuje se obuka i testiranje iz oblasti zaštite tri puta godišnje. Merenjem usaglašenosti prakse, politike i standarda zaštite, organizacija, u slučaju potrebe, dokazuje pravosudnim organima i poslovnim partnerima, da štiti svoje informacije i efikasno upravlja sistemom zaštite, što uliva veće uzajamno poverenje.

Interni nadzor, kontrola i tehnička revizija sistema zaštite, igraju ključnu ulogu u zaštiti kiber prostora i olakšavaju eksternu reviziju. Cilj je evaluirati efektivnost sistema zaštite, *proaktivno* inicirati novu procenu rizika i razvoj strategije za ublažavanje rizika. *Učestalost nadzora, kontrole i revizije* zasniva se na zdravoj logici: što su veći faktori rizika i vrednost imovine, ona treba da bude češća. Od velike je pomoći *metod* skeniranja za automatsku procenu ranjivosti i oporavak IKTS. *Obim nadzora, kontrole i revizije* mora biti pažljivo definisan i treba verifikovati brojne komponente, procese i dokumenta zaštite. Preporuke standarda zaštite (ISO/IEC 27001) su da se najmanje jednom godišnje procenjuje rizik, a na osnovu te procene pravi plan za interni nadzor, kontrolu i reviziju. Preporučuju se rutinske vežbe i simulacije kompjuterskog incidenta i vanrednog događaja, čime se *ističe značaj nadzora, kontrole i revizije, obezbeđuju prioriteti zaštite i upravljanje kompjuterskim incidentom različitog nivoa intenziteta.*

Nezavisna (eksterna) revizija (*audit*) najčešće se vrši u fazi reinženjeringa IKTS u cilju povećanja produktivnosti i smanjenja troškova poslovanja. Uključivanje spoljnih revizora unosi dodatni rizik, koji se mora razmatrati. Spoljna revizija se mora izvršiti u bezbednom okruženju i atmosferi poverenja, uz obavezno prisustvo internog revizora i odobrenje glavnog menadžera.

Nametanje obaveze sprovođenja politike zaštite je kritičan faktor uspeha. Revizija sistema zaštite je u suštini u ovoj funkciji. *Izveštaj revizora* deo je dokumentacije zaštite, a može se koristiti da *pokaže mertrički sistem revizora, pomogne u planiranju, izvršavanju i kontroli procesa revizije, olakša kontrolu rada nezavisnog revizora, evaluira sistem kvaliteta procesa revizije, obezbedi podršku u slučaju naplate polise osiguranja ili sudskog gonjenja itd.* [21]. U *Izveštaju o reviziji* treba obraditi pitanja kao što su: *zaštićenost sistemskih i aplikativnih programa, ažurnost i usaglašenost politike i drugih dokumenata zaštite, adekvatnost i prihvatljivost manuelnog/ automatizovanog sistema revizije, format izveštaja o reviziji, svest o potrebi* itd.

Revizorski izveštaj je ulazna informacija za reinženjering i korekciju slabih tačaka sistema zaštite. Sankcije za nesprovođenje politike zaštite moraju biti unapred planirane, jer nema smisla implementirati sistem zaštite, ako se povrede ignorišu.

14 David J. Lineman**,** *The New ISO 17799:2005 – Security Policy Implications For Business,* Information Shield Policy, 2010.

1.4. REZIME

Bezbednost informacija u IKTS je *objektivna mera/ocena* stanja rizika ili stanja sigurnog, pouzdanog i neometanog funkcionisanja IKTS, u odnosu na sam sistem i njegovo okruženje. Sistem se smatra bezbednim, ako je *zaštićen* od uticaja faktora rizika. *Sigurnost IKTS* je sinonim *bezbednosti*, *subjektivna mera* uverenja korisnika da je sistem bezbedan. *Nivo bezbednosnog stanja* određen je nivoom preostalog prihvatljivog rizika. Ukupna bezbednost proporcionalna je skupu bezbednosnih stanja svih komponenti, koje neravnomerno, aditivno utiču na ukupnu bezbednost, a najveći uticaj imaju najosetljivije komponente sistema bezbednosti.

Bezbednost IKTS je konkretno, situacioni problem stanja sistema i realnog okruženja i ne postoji univerzalno i nepromenljivo stanje bezbednost IKTS. U realnim uslovima, sa porastom pretnji nivo ukupne bezbednosti IKTS nelinearno opada, zbog stohastičke prirode pretnji. *Održavanje stanja bezbednosti* IKTS, na prihvatljivom nivou rizika, obezbeđuje implementirani *sistem zaštite* poverljivosti, integriteta i raspoloživosti informacija–*organizovan i koherentan skup U, O i T kontrola zaštite i njihovih veza i ograničenja, primenjenih na IKTS, radi zaštite raspoloživosti, poverljivosti i integriteta informacija i namenjenog funkcionisanja IKTS u izvršavanju poslovnih ciljeva i misije organizacije*.

Osnovnu funkcionalnost sistema zaštite čine *servisi zaštite,* koji se implementiraju izvršavanjem skupa bezbednosnih funkcija. Bezbednosne funkcije vrše *mehanizmi i protokoli* zaštite: pojedinačni algoritmi, hardversko-softverski moduli i metodi. Za upravljanje mehanizmima zaštite obezbeđene su određene kontrolne strukture ili *kontrole zaštite,* koje obuhvataju *U, O i T* kontrole.

Sa aspekta zaštite, osnovni zahtev je *smanjenje kompleksnosti,* što se postiže sistem -inženjerskim, *objektno-orijentisanim i procesnim pristupom* u svim fazama razvoja IKTS. Smanjenje kompleksnosti počinje uvođenjem *grana informacionih objekata* zaštite: *raspoloživost, integritet i poverljivost* informacija*,* čime se struktuira bezbednosni cilj i *grana objekata za zaštitu*: *U*, *O i T kontrole zaštite*, koje struktuiraju sredstava za postizanje bezbednosnog cilja.

U generičkom modelu sistem zaštite štiti informacionu imovinu od pretnji, malicioznih i namernih napada. *Kontrole zaštite* se implementiraju da redukuju ranjivosti i izloženost IKTS u skladu sa rezultatima procene rizika i zahtevima *politike zaštite*. Preostali rizik, na prihvatljivom nivou, vlasnik sistema nastoji smanjiti u cikličnom procesu zaštite. Cilj svakog programa zaštite informacija je da razvije *optimalan sistem* zaštite, koji u datim uslovima na najbolji način zadovoljava sve uslove, a postiže se putem najracionalnije raspodele resursa utrošenih na rešavanje zadataka zaštite.

Savremeni *web* servisi (*web* aplikacije, SOA, *Cloud Computing* i dr.) i e-poslovanje zahtevaju promenu paradigme klasične zaštite IKTS, sa rešenjima *distribuiranih* mehanizama zaštite, koji se ne samo implementiraju, nego i *ugrađuju* u hardverske i softverske komponente u toku njihovog razvoja.

U praksi zaštite primenjuju se dva glavna metoda za implementaciju sistema zaštite od dinamički promenljivih pretnji: *sveobuhvatnim smanjenjem ukupnog rizika na prihvatljivi nivo*, što zahteva velike resurse i *procesom 4-fazne tranzicije iz jednog u više bezbednosno stanje*, koji preporučuje metod OCTAVE. U 1. fazi obezbeđuje se zaštita objekata kritičnih za misiju organizacije od glavnih faktora rizika, a u sledećim fazama progresivno razvija program zaštite od ostalih faktora rizika. Generički proces implementacije sistema zaštite odvija se u četiri faze: (1) priprema i izbor tima, (2) identifikovanje internih i eksternih faktora rizika, (3) nadzor, kontrola i revizija i (4) usaglašavanje programa zaštite.

Svaki proces implementacije programa zaštite može biti različit u organizacijama, ali treba da obuhvata tri obavezne komponente: *obuku zaposlenih, kontrolu usaglašenosti* i *nametanje obaveze izvršavanja* politike i procedura zaštite. Obuka treba da obuhvati sve strukture zaposlenih. Usaglašenost obuhvata *opštu usaglašenost* programa i politike zaštite sa zakonima i standardima i *specifičnu usaglašenost* prakse i politike zaštite. Obaveze sprovođenja programa i politike zaštite nameće se merama internog nadzora, kontrole i revizije i eksterne revizije (*auditing*), obaveznog izveštavanja o bezbednosno relevantnim događajima i sankcionisanja nesprovođenja politike zaštite.

1.5. KLJUČNI TERMINI

Arhitektura sistema zaštite: funkcionalni odnosi komponenti sistema zaštite.

Bezbednost*:* objektivna mera**/**ocena stanja sistema u odnosu na samog sebe ili okruženje. *Sinonim:* sigurnost.

IKTS: sistem IKT, koji obuhvata integrisani skup ljudi, programa, hardvera, protokola, komunikacione infrastrukture, procesa i njihovih međusobnih veza. *Sinonim: IS*.

Informacija: podaci o činjenicama, saznanjima, procesima i pojavama, o stanju objekata u nekoj predmetnoj oblasti; skup podataka koji donosi novo saznaje.

Informaciona imovina: obuhvata *čistu informacionu imovinu* (digitalni podaci i informacije, aplikativni i sistemski programi), *fizičku* (infrastruktura za podršku i kontrolu okruženja IKTS, hardver i ostala imovina IKTS) i *humanu* (zaposleni i nezaposleni).

Integritet informacija, sistema: stanje u kojem informacije/sistemi nisu izmenjeni na neovlašćen način.

Kontrole zaštite: upravljački okvir mehanizama i protokola zaštite; grupišu se u klase upravljačkih, operativnih i tehničkih kontrola; interfejs između mehanizma zaštite i čoveka.

Korisnik IKTS: lice/grupa/program korisnika IKTS sa pravima pristupa i korišćenja servisa.

Mehanizmi i protokoli zaštite: pojedinačni algoritmi, hardversko–softverski moduli i metodi za izvršavanje bezbednosnih funkcija; u logičkom smislu realizuju servise zaštite.

Model: aproksimacija realnog sistema, koja približno predstavlja tokove procesa, funkcionisanje i/ili druge relevantne atribute realnog sistema.

Neporecivost informacija: stanje sistema u kojem stranke u transakciji ne mogu naknadno poricati izvršene aktivnosti u transakciji ili delovima transakcije.

Objekti zaštite: fizički, logički i humani objekti informacione imovine, koje štiti sistem zaštite.

Optimalni sistem zaštite: sistem zaštite u kojem su troškovi kontrola zaštite potpuno izjednačeni sa procenjenim potencijalnim gubicima.

Plan zaštite: sveobuhvatan strateški dokument za zaštitu informacija; predstavlja plan implementacije programa, politike i procedura zaštite.

Politika zaštite IKTS: izjava na nivou IKTS koja obezbeđuje okvir očekivanog i obaveznog ponašanja upravne strukture, zaposlenih, tehnologije i procesa. **Procedure zaštite:** Precizno definisani načini primene elemenata politike zaštite sa listom detalja i specifičnih koraka koje pojedinci moraju sprovoditi.

Pouzdanost (*funkcionalna*, *tehnička*, *operativna***)**: korektno funkcionisanje komponenti i sistema u operativnom okruženju, sa performansama u propisanim granicama.

Poverljivost informacija/sistema: stanje u kojem su informacije/sistemi nedostupni neovlašćenim korisnicima.

Program zaštite: sveobuhvatan skup aktivnosti za zaštitu informacione imovine organizacije; predstavlja smernice za izradu, politike, procedura i plana zaštite.

Raspoloživost informacija/sistema: stanje u kojem se informacijama/sistemima može pristupati po potrebi.

Servis zaštite: logičke aplikacione jedinice, koje se izvršavaju kroz različite akcije, izvršavanjem *mehanizama* i *protokola zaštite*.

Sigurnost sistema: mera subjektivnog osećaja/uverenja da je sistem bezbedan, da mu ne preti nikakva opasnost, jer je zaštićen. *Sinonim*: bezbednost sistema.

Sistem zaštite: organizovan i koherentan skup **U, O** i **T** kontrola zaštite i njihovih veza i ograničenja, primenjenih na IKTS da bi se zaštitila CIA informacija.

1.6. PITANJA ZA PONAVLJANJE

1. Tendencija je da se terminologija zaštite informacija što je moguće više učini:
   a. kompleksnom i nerazumljivom za krajnje korisnike iz bezbednosnih razloga
   b. jasnom i razumljivom za sve korisnike
   c. jasnom i razumljivom samo za specijaliste zaštite
   d. nejasnom i nerazumljivom za menadžere organizacije
2. Bezbednost IKTS je:
   a. objektivna mera/ocena stanja rizika IKTS
   b. subjektivna ocena stanja zaštićenosti IKTS
   c. funkcionalna komponenta IKTS
   d. ni jedan od navedenih odgovora
3. Nivo ukupne bezbednosti složenog sistema (Bu):
   a. raste približno linearno i aditivno sa porastom nivoa bezbednosti njenih relativno nezavisnih bezbednosnih komponenti (B1, B2, ..., Bn)
   b. raste približno nelinearno i multiplikativno sa porastom nivoa bezbednosti njenih relativno nezavisnih bezbednosnih komponenti (B1, B2, ..., Bn)
   c. raste približno nelinearno i aditivno sa porastom nivoa bezbednosti njenih relativno nezavisnih bezbednosnih komponenti (B1, B2, ..., Bn)
4. Funkcija zavisnosti komponenti bezbednosti IKTS–Bi od faktora rizika–Ri je:
   a. linearno opadajuća
   b. linearno rastuća
   c. nelinearno opadajuća
   d. eksponencijalno opadajuća
5. Stabilno održavanje stanja bezbednosti IKTS na određenom nivou, najtačnije obezbeđuje:
   a. tim specijalista za zaštitu
   b. sistem servisa i kontrola osnovne zaštite
   c. održavanje rizika na prihvatljivom nivou
   d. tim za zaštitu i implementirani sistem za zaštitu
6. Na bezbednosno stanje IKTS utiču sledeći ključni faktori:
   a. korisnički zahtevi i politika zaštite
   b. funkcionalni zahtevi i organizaciona struktura IKTS
   c. kadrovska struktura i ugled organizacije
   d. razvoj tehnologija i malicioznih programa
   e. razvoj standarda i normativa zaštite
   f. kompleksnost IKTS i terminologije zaštite
7. Sa aspekta kvaliteta, nužno je i dovoljno obezbediti sledeća svojstva informacija:
   a. blagovremenost, tačnost, korisnost
   b. poverljivost, integritet, raspoloživost
   c. blagovremenost, tačnost, integritet
   d. poverljivost, tačnost, integritet, raspoloživost
   e. blagovremenost, integritet, raspoloživost
8. Sistem zaštite najbolje objašnjava izraz:
   a. aditivna funkcija intenziteta vektora zaštite
   b. skup funkcija zaštite sa kojim se izvršavaju određeni bezbednosni zadaci
   c. multiplikativna funkcija intenziteta vektora zaštite
   d. organizovan i koherentan skup upravljačkih, organizaciono–operativnih i tehničkih kontrola zaštite
9. Optimalni sistem zaštite je sistem, koji u datim uslovima:
   a. na najbolji način zadovoljava sve bezbednosne zahteve, sa racionalnim resursima za akviziciju, implementaciju i održavanje sistema zaštite
   b. ne zadovoljava sve bezbednosne zahteve, ali se postiže se neznatnim resursima za akviziciju, implementaciju i održavanje sistema zaštite
   c. zadovoljava sve bezbednosne zahteve, ali se postiže se značajnim resursima za akviziciju, implementaciju i održavanje sistema zaštite

10. Servis zaštite je:
    a. logička aplikaciona jedinica, koja se izvršava kroz različite akcije, izvršavanjem *mehanizama* i *protokola zaštite*
    b. hardversko–softverski modul za izvršavanje bezbednosnih funkcija
    c. konačna klasifikacija mehanizama zaštite i interfejs prema korisniku
11. Mehanizam zaštite je:
    a. proces ili neprekidna aktivnost, koja se izvršava izvršavanjem bezbednosnih funkcija kontrola zaštite
    b. hardversko–softverski modul za izvršavanje bezbednosnih funkcija
    c. interfejs prema korisniku servisa zaštite
12. Kontrola zaštite je:
    a. proces ili neprekidna aktivnost, koju vrše bezbednosne funkcije mehanizama zaštite
    b. hardversko–softverski modul za izvršavanje bezbednosnih funkcija
    c. konačna klasifikacija mehanizama zaštite i interfejs između mehanizma zaštite i čoveka
13. Dva glavna metoda za implementaciju programa zaštite su:
    a. metod životnog ciklusa sistema i metod vodopada
    b. sveobuhvatno ublažavanje ukupnog rizika na prihvatljiv nivo i metod četverofazne tranzicije iz jednog u drugo bezbednosno stanje
    c. iterativni metod i metod brzog odgovora
14. U objektno orijentisanom pristupu za smanjenje kompleksnosti uvode se grane objekata:
    a. informaciono komunikacionog sistema
    b. informacione imovine ili CIA informacija
    c. računarske mreže i web servisa
    d. mera i sredstava zaštite ili proceduralnih i tehničkih kontrola zaštite
15. Čista informaciona imovina obuhvata:
    a. digitalni podaci i informacije, opipljiva informaciona imovina, neopipljiva informaciona imovina, aplikativni program, sistemski program
    b. infrastruktura za podršku IKTS, kontrole okruženja IKTS, hardver IKTS, imovina IKTS
    c. aplikativni program, sistemski program, infrastruktura za podršku IKTS
    d. zaposleni, ne-zaposleni, spoljni saradnici, poslovni partneri
    e. zaposleni, ne-zaposleni
16. Fizička imovina obuhvata:
    a. digitalni podaci i informacije, opipljiva informaciona imovina, neopipljiva inf. imovina, aplikativni program, sistemski program
    b. infrastruktura za podršku IKTS, kontrole okruženja IKTS, hardver IKTS, imovina IKTS
    c. aplikativni program, sistemski program, infrastruktura za podršku IKTS
    d. zaposleni, ne-zaposleni, spoljni saradnici, poslovni partneri
    e. zaposleni, ne-zaposleni
17. Humana imovina obuhvata:
    a. digitalni podaci i informacije, opipljiva informaciona imovina, neopipljiva inf. imovina, aplikativni program, sistemski program
    b. infrastruktura za podršku IKTS, kontrole okruženja IKTS, hardver IKTS, imovina IKTS
    c. aplikativni program, sistemski program, infrastruktura za podršku IKTS
    d. zaposleni, ne-zaposleni, spoljni saradnici, poslovni partneri
    e. zaposleni, ne-zaposleni
18. Relevantni aspekti zaštite IKTS, koje treba razmatrati kao objekte zaštite obuhvataju:
    a. ključne karakteristike pretnji, servisi IKTS, kvalitet IKTS servisa
    b. ključne karakteristike IKTS, servisi IKTS, kvalitet IKTS servisa
    c. ključne karakteristike IKTS, servisi zaštite IKTS, kvalitet IKTS servisa
    d. ključne karakteristike IKTS, servisi IKTS, kvalitet servisa zaštite
19. Generički model sistema zaštite obuhvata sledeće objekte:
    a. vlasnik IKTS, agent pretnje, sistem

zaštite, pretnja, CIA informacija, procena rizika, kontrole zaštite, ranjivosti, izloženost,
   b. politika zaštite, preostali rizik, prihvatljivi nivo rizika, evaluacija, sertifikacija i akreditacija, SOA
   c. administrator IKTS, preostali rizik, prihvatljivi rizik, evaluacija, sertifikacija i akreditacija, SOA
   d. vlasnik IKTS, servisi zaštite, pretnje, topologija RM, procena rizika, kontrole zaštite, ranjivosti, izloženost, politika zaštite, dokument SOA

20. U zaštiti savremenih IKTS bazična je primena sledeća dva principa:
   a. odbrana po dubini i primarna zaštita najvrednije informacione imovine
   b. odbrana po dubini i prstenovi zaštite
   c. virtuelizacija i prstenovi *slojeva luka*
   d. digitalni mravi i prstenovi *slojeva luka*
21. U zaštiti savremenih IKTS nova paradigma zaštite obuhvata sledeće tehnologije:
   a. odbrana po dubini i primarna zaštita najvrednije informacione imovine
   b. odbrana po dubini i prstenovi zaštite
   c. virtuelizacija i prstenovi *slojeva luka,* proaktivna zaštita
   d. digitalni mravi, prstenovi *slojeva luka,* IDPS, proaktivna zaštita
22. Generičke tok procesa implementacije sistema zaštite obuhvata sledeće faze:
   a. priprema (definisanje obima i granice projekta i izbor tima)
   b. stalni nadzor i interna revizija
   c. identifikovanje bezbednosnih faktora rizika
   d. sertifikacija i akreditacija sistema zaštite
   e. revizija efikasnosti sistema zaštite i preporuke za izmenu
   f. integracija i prilagođavanje kontrola zaštite u skladu sa nalazima revizije
23. Obavezne komponente sadržaja svakog procesa implementacije sistema zaštite:
   a. obuka zaposlenih, nadzor i revizija usaglašenosti i nametanje obaveze sprovođenja politike
   b. obuka zaposlenih i nametanje obaveze izvršavanja politike zaštite
   c. obuka zaposlenih, kontrola pristupa, akreditacija i sertifikacija sistema
24. Potencijalno korisne upotrebe izveštaja o reviziji sistema zaštite su (*ISACA*) da:
   a. evaluira politiku zaštite i sistem kvaliteta procesa revizije
   b. demonstrira metrički sistem i pomogne u planiranju i izvršavanju revizije
   c. olakša kontrolu rada IKTS i obezbedi izradu plana zaštite
   d. obezbedi podršku u slučaju naplate polise osiguranja ili sudskog gonjenja
25. Nametanje obaveze sprovođenja programa/politike zaštite je:
   a. kritičan faktor uspeha programa/politike zaštite i u funkciji revizije sistema zaštite
   b. značajan za uspeh programa/politike zaštite, ali ne zavisi od revizije zaštite
   c. kritičan faktor uspeha programa/politike zaštite, a revizija je u toj funkciji
   d. nije kritičan faktor uspeha programa/politike zaštite, a revizija je u toj funkciji

2. PRINCIPI, STANDARDI I NORMATIVI ZAŠTITE

Po završetku ovog poglavlja razumećete:

- Koncept i značaj principa, standarda i normativa zaštite
- Sistemske i opšte prihvaćene principe zaštite (GAISP)
- Funkcionalne i detaljne principe zaštite (GAISP)
- Interne i eksterne standarde zaštite
- Ključne standarde za upravljanje zaštitom (ISO/IEC 27001...)
- Normativni okvir zaštite informacija

2.1. UVOD

Kompleksni sistem zaštite informacija uključuje *principe*, *standarde, normative*, *praksu* i *tehnologije* na kojim su zasnovani. Za harmonizaciju sistema zaštite, potrebna je koordinacija svih ovih faktora. *Princip* je fundamentalna istina ili zakonitost, koja se uzima bez dokazivanja kao osnova za izvršavanje racionalne aktivnosti. Generalno prihvaćeni principi zaštite informacija – GAISP (*Generally Accepted Information Security Principles),* nastali su saradnjom ekspertskih timova iz više zemalja (EU, SAD, Kanade, Australije itd.) i na osnovu brojnih standarda (OECD, NIST, ISO/IEC 17799, ISO/IEC 27001, COBIT i dr.). GAISP *principi zaštite* se ažuriraju svake tri godine i impliciraju da *svaki princip u određenom slučaju može imati izuzetak*. Specijalisti zaštite ih koriste u svim fazama životnog ciklusa sistema zaštite, proizvođači u proizvodnji komponenti/uređaja, a vlasnici i menadžeri za razvoj programa zaštite. GAISP principi se odnose na fizičke, tehničke, personalne i proceduralne komponente, a dele na *opšte* - za upravljanje zaštitom, *funkcionalne* - za operativno upravljanje komponentama sistema zaštite i *detaljne* - za upravljanje mehanizmima zaštite. Konzistentni principi zaštite su osnovni gradivni elementi procesa zaštite.

Standardi zaštite obezbeđuju široko prihvaćena pravila za upravljanje zaštitom informacija, a mogu se izvoditi iz normativa (Zakoni i podzakonska akta) ili industrijskih standarda najbolje prakse zaštite. Pomažu korisnicima da prevedu zahteve za zaštitu iz normativa u zahteve politike zaštite. *Normativi* u oblasti zaštite obezbeđuju osnovni okvir za šire uspostavljanje i implementaciju programa zaštite IKTS u organizacijama, kao i mehanizme sankcionisanja koji motivišu korisnike da ih sprovode. Principi, standardi i normativi zaštite čine metodološku osnovu za izradu *dokumenata zaštite*.

2.2. SISTEMSKI PRINCIPI ZAŠTITE

Sistemski principi zaštite su preuzeti iz procesa upravljanja IKTS (što implicira termin „*sistemski*")**.** Obuhvataju opšte prihvaćene i u praksi dokazane personalne, organizacione i operativne mere u IKTS, koje sprečavaju sukob nadležnosti i interesa, zloupotrebu privilegija i povećavaju opštu pouzdanost resursa IKTS. Efektivni su mehanizmi za održavanje pouzdanog rada sistema i baza za implementaciju GAISP principa [27,43,64]. *Sistemski* principi su obavezan okvir u koji se ugrađuju specifični GAISP principi zaštite i obuhvataju principe [61]: *„nikada sam", rotaciju radnih mesta, razdvajanje dužnosti, minimum privilegija, znati samo što je potrebno i principe upravljanja IKTS*.

Princip „nikada sam" sprečava monopolski položaj i obezbeđuje samokontrolu u IKTS i zahteva zapošljavanje najmanje dva lica, za sledeće bezbednosno relevantne poslove: *autorizaciju prava pristupa; procesiranje osetljivih informacija; testiranje i prijem hardvera i softvera; modifikaciju hardvera, softvera i IKTS; projektovanje i implementaciju baze podataka, sistemskih, aplikativnih i programa za zaštitu; izmenu dokumentacije i procedura u IKTS; destrukciju važnih programa itd*.

Rotacija radnih mesta zahteva da ni jedno lice ne ostane na nekom bezbednosno značajnom mestu u IKTS toliko dugo da pomisli da je nezamenljiv. Rotacija osoblja se preporučuje, ali zavisi od broja zaposlenih i kvalifikovanih lica.

Razdvajanje dužnosti zahteva da ni jedno lice istovremeno ne može obavljati dve ili više od deset sledećih parova funkcija u IKTS**:**

1. operativni rad na računaru – programiranje;
2. unos i priprema podataka za obradu – obrada podataka;
3. obrada podataka – kontrola kvaliteta IKTS;
4. operativni rad na računaru – čuvanje elektronskih medija;
5. prijem osetljivih informacija – predaja osetljivih informacija;
6. kopiranje, izdavanje/uništavanje osetljivih informacija – izdavanje ovlašćenja;
7. programiranje aplikacija – sistemsko programiranje;
8. programiranje aplikacija – administracija baza podataka;
9. projektovanje, implementacija/modifikacija sistema zaštite - bilo koji drugi;
10. kontrola ovlašćenja za pristup – bilo koji drugi posao.

U manjim IKTS, uprkos sistemskom principu razdvajanja dužnosti, u porastu je tendencija konvergencije dužnosti administratora sistema i administratora zaštite.

Princip minimuma privilegija znači davanje što je moguće manje privilegovanih naloga za pristup objektima IKTS.

Princip znati samo što je potrebno znači davanje prava pristupa samo informacijama potrebnim za obavljanje posla.

Princip upravljanja IKTS obezbeđuje osnovni nivo upravljanja zaštitom, a obuhvata *postavljanje fizičkih prepreka i ograničenja i administrativno nametanje pravila ponašanja u radu sa IKTS*. *Fizička ograničenja*, uključuju: bezbedno čuvanje elektro-optičkih medija; pripremu osetljivih podataka za obradu u restriktivnom prostoru; odvojenu radnu sobu programera od serverske sobe; zabranu pristupa u sobu administratora zaštite za sve osim zaposlenih u zaštite; skladištenje otpada za uništavanje na bezbedno mesto izvan serverske sobe i dr. Administrativno upravljanje zaštitom uključuje upravljanje korisničkim nalozima za pristup IKTS.

Takođe, moguće je naći vezu između opštih principa zaštite informacija i biologije, kao što su koncepti malicioznih programa – virusa i crva i trofazni koncept *prevencije, detekcije i kontrole*, koji se koriste u biologiji i zaštiti informacija.

2.3. OPŠTE PRIHVAĆENI PRINCIPI ZAŠTITE

2.3.1. Namena GAISP principa zaštite

Osnovna namena GAISP principa zaštite je da pomogne vlasnicima informacija za upravljanje, specijalistima zaštite za razvoj sistema zaštite, a proizvođačima za proizvodnju komponenti i uređaja zaštite. GAISP principi imaju višestruku upotrebljivost i koriste se da [27,43]: *promovišu najbolju praksu zaštite; obezbede referentne principe usaglašenih mišljenja i prakse zaštite; motivišu poslovne sisteme i uvere menadžere da je zaštita konzistentna i merljiva; povećaju kontrolu i bezbednost operativnog okruženja; smanje troškove zaštite; omoguće sertifikaciju sistema i izradu politike zaštite; povećaju efektivnost servisa i specijalista zaštite; povećaju poverenje u proizvode zaštite; ubrzaju razvoj metodologija i tehnologija zaštite itd*.

2.3.2. Struktura GAISP principa zaštite

GAISP principi su sveobuhvatna hijerarhija instrukcija za obezbeđenje opšte prihvaćenog okvira za zaštitu IKTS, koji uključuje *osnovne* – na upravljačkom, *funkcionalne* – na operativnom i *detaljne* – na tehničkom nivou. *Osnovni* GAISP principi usmeravaju menadžment i pomažu organizaciji da definiše efektivnu strategiju zaštite. *Funkcionalni* GAISP principi, su gradivni blokovi osnovnih i detaljnije definišu taktiku izgradnje efektivne arhitekture sistema zaštite. *Detaljni* GAISP principi su namenjeni za profesionalce u zaštiti, a koriste funkcionalne principe kao okvir i obezbeđuju specifična, sveobuhvatna uputstva za dnevne aktivnosti u procesima upravljanja rizikom i sistemom zaštite.

U praksi zaštite, treba obezbediti da je svaki GAISP princip precizno definisan, kompletan i konzistentan, usaglašen sa bezbednosnim ciljem, tehnički racionalan i prihvatljiv, dobro prezentiran, gramatički korektan i jezički razumljiv i usklađen sa primenljivim standardima i uputstvima zaštite.

GAISP principi zaštite su struktuirani i opisani u standardnom formatu – *naziv, definicija, objašnjenje (opis) i primer principa*, kao na primer:

Ime: *kontrolisana odgovornost (accountability) za logičku kontrolu pristupa.*

Definicija: *ovlašćenja i odgovornosti za pristup moraju u sistemu zaštite biti jasno definisani, shvaćeni, lično prihvaćeni i kontrolisani*.

Objašnjenje: *kontrolisana odgovornost omogućava da se kontrolišu akcije svih učesnika koji interaktivno rade u IKTS. Uloge i odgovornosti se jasno definišu, identifikuju i dodeljuju ovlašćenja pristupa osetljivim i kritičnim informacijama, zaposlenim na svim nivoima organizacije. Odnosi između učesnika, procesa i informacija moraju biti jasno definisani, dokumentovani i prihvaćeni od svih učesnika, koji moraju preuzeti odgovornosti.*

Primer: *na osnovu pregleda i analize bezbednosno relevantnih događaja u log datoteci sistema, treba izvršiti reviziju kritičnih informacija. Log datoteka sadrži sve izmene informacija.*

2.3.2.1. Opšti GAISP principi zaštite

Opšti GAISP principi (tabela 2.1) pomažu organizaciji da definiše efektivnu strategiju zaštite.

Tabela 2.1. Opšti GAISP principi zaštite

GAISP princip	Opis
Svesti o potrebi zaštite	svi relevantni učesnici treba da budu svesni primenljivih pretnji za bezbednost IKTS i tehnologija zaštite informacija.
Odgovornosti	ovlašćenja i odgovornosti moraju u sistemu zaštite biti jasno definisani, shvaćeni, prihvaćeni i kontrolisani.
Stalnog preispitivanja	rizik za informacionu imovinu mora se regularno periodično procenjivati, a procesi zaštite neprekidno unapređivati.
Demokratičnosti	u procesima zaštite treba jednako uvažavati privatnost, lična i autorska prava i dostojanstvo svih učesnika.
Etičkog ponašanja	informacije koje se štite treba da budu etički prihvatljive, a administriranje zaštite u skladu sa opštim kodeksom ponašanja.
Integracije	principi, standardi i mehanizmi treba da budu komplementarni i sinergijski integrisani u politiku, procedure i kontrole zaštite.
Multidisciplinarnosti	principi, standardi i mehanizmi zaštite treba da sveobuhvatno uključuju sve relevantne aspekte različitih disciplina.
Proporcionalnosti	kontrole zaštite treba projektovati, implementirati i primenjivati za zaštitu informacija, proporcionalno proceni rizika.
Blagovremenosti	sve komponente zaštite treba da blagovremeno sprečavaju napade na IKTS.

Po svojoj prirodi su fundamentalni, retko se menjaju i obuhvataju zaštitu CIA informacija. Objavio ih je komitet OECD, a prihvatio NIST sa neznatnim proširenjem.

2.3.2.2. Funkcionalni GAISP principi zaštite

Funkcionalni principi zaštite brojniji su i detaljniji od opštih, čine okvir za razvoj još brojnijih, detaljnih principa, a menjaju se sa glavnim promenama okruženja i tehnologija zaštite. Predstavljaju gradivne blokove osnovnih principa zaštite, definišu preporuke za implementaciju i operativnu primenu kontrola zaštite, a čine ih sledeći principi: politika zaštite, obuka i razvoj svesti o potrebi zaštite, odgovornost, upravljanje informacionom imovinom, upravljanje fizičkom i zaštitom okruženja, upravljanje personalnom zaštitom, upravljanje incidentom, upravljanje zaštitom u životnom ciklusu IKTS, kontrola pristupa, upravljanje vanrednim događajem i kontinuitetom poslovanja, upravljanje bezbednosnim rizikom, zaštita mreže od rizika sa Interneta, normativni, administrativni i ugovorni zahtevi, etički principi itd.

2.3.2.3. Detaljni GAISP principi zaštite

Detaljne GAISP principe definišu i primenjuju specijalisti zaštite u dnevnom radu. Oni čine osnovne elemente *procedura zaštite* i često se menjaju sa promenama tehnologija. Sadrže detaljna objašnjenja i podržavaju jedan ili više funkcionalnih GAISP principa. Usaglašavaju se sa funkcionalnim principima, uključujući nove tehnologije i pretnje. Na primer, detaljni *princip kontrole pristupa* podržava funkcionalni princip – *kontrolu pristupa,* koji, pak, podržava opšti princip – *proporcionalnosti*, a opisuje se u formi:

Ime*: detaljni princip kontrole pristupa*.

Definicija: koristiti *jednokratne lozinke* za logičku kontrolu pristupa svim informacijama. koje se smatraju kritičnim za organizaciju.

Objašnjenje: višestruko korišćene lozinke su tradicionalno jedina tehnika na raspolaganju za kontrolu pristupa objektima IKTS. Tehnološke promene učinile su lozinke za višekratnu upotrebu zastarelim u brojnim primenama. Za kontrolu pristupa i autentifikaciju uvodi se lozinka za jednokratnu upotrebu, koju omogućava tehnologija *smart* kartica.

Primer: primena smart kartice za ulazak u zgradu, radnu prostoriju i pristup računaru.

2.4. STANDARDI ZAŠTITE

2.4.1. Generička definicija standarda zaštite

Prva faza razvoja standarda zaštite je razvoj RFC (*Request For Comment*) specifikacija [78, 79]. Kada RFC specifikacija postane razumljiva, stabilna i tehnički kompetentna, može postati standard zaštite, kroz prelazne forme *nacrta* i *de facto* standarda. Telo za standardizaciju IETF (*Internet Engineering Task Force*) objavljuje RFC po odobrenju IESG (*Internet Engineering Steering Group*) [39].

Standard zaštite je usvojen i objavljen dokument koji uspostavlja specifikaciju i procedure, dizajnirane da obezbede da dokumenta, materijali, proizvodi, metodi ili servisi zaštite, odgovaraju nameni i konzistentno izvršavaju predviđene funkcije. U praksi, standard zaštite sadrži čitav set aranžmana za pokrivanje što većeg broja tipičnih bezbednosnih zahteva za održavanje rizika na prihvatljivom nivou. Standardi zaštite obezbeđuju preporuke za razvoj, implementaciju i održavanje sistema zaštite i glavni je alat za poboljšanje kvaliteta kontrola zaštite, integrisanjem delova standarda u poslovne procese, procenu kvaliteta i izbor kontrola zaštite, poboljšanje programa obrazovanja, obuke i razvoja svesti o potrebi zaštite itd. Bitni atributi kvaliteta svakog standarda su, da je: *dokumentovan, raspoloživ, sveobuhvatan, izdat od strane nacionalnog tela za standardizaciju, adekvatan nameni, rentabilan, dobrovoljno prihvaćen, usaglašen sa zakonima i da obezbeđuje indikatore progresa* [64].

Standardi zaštite uvode promene u upravljački okvir sistema zaštite. Primarni cilj standarda zaštite *nije sama standardizacija sistema zaštite*, što bi se moglo lako zloupotrebiti. Potpuno standardizovana zaštita sigurno bi izazvala znatno veći broj napada i pokušaja proboja, a to bi moglo ugroziti i sam koncept zaštite.

2.4.2. Opšti model standarda zaštite

Opšti, hijerarhijski model standarda zaštite uključuje *terminologiju, principe, metodologiju, elemente standarda, uputstvo i dodatke za primenu, tehnike i alate* (sl. 2.1).

Terminologija uključuje listu definicija i pojmova. *Principi* obezbeđuju generalno prihvatljiva, aksiomatska pravila za izradu uputstava zaštite. *Metodologija*



Sl. 2.1. Opšti model standarda zaštite informacija [61]

(okvir) obezbeđuje pojednostavljen opis načina korišćenja koncepta, metoda i tehnika i njihovih međusobnih odnosa. *Elementi standarda* obezbeđuju specifične zahteve za definisanu komponentu zaštite. *Uputstvo* obezbeđuje detaljniji opis primene elemenata standarda u specifičnim situacijama. *Tehnike i alati* podržavaju primenu standarda [61].

2.4.3. Tela za standardizaciju zaštite

Standardi postoje za komponente i sisteme zaštite, organizacije i profesionalce koji se bave zaštitom, tako da organizacije, proizvodi i profesionalci zaštite mogu biti sertifikovani i akreditovani prema određenom standardu. Standarde donose brojna međunarodna, akreditovana tela (tabela 2.2).

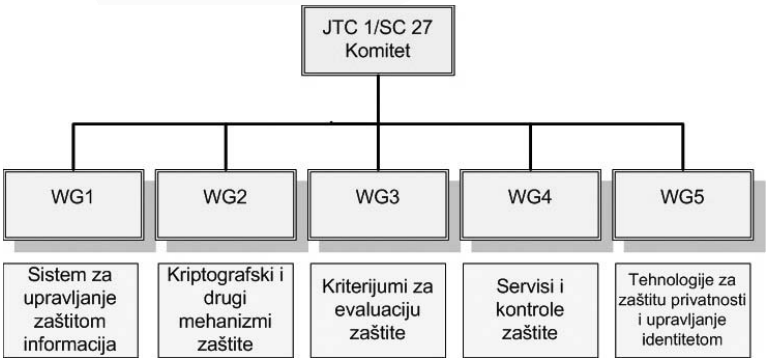
Tabela 2.2. Relevantna međunarodna tela za standardizaciju u oblasti zaštite

Međunarodna standardizaciona tela u oblasti zaštite informacija	
BSI	*British Standards Institute*
BSI (German)	*Bundesamt fuer Sicherheit in der Informationstechnik*
ISO	*International Organization for Standardization*
IEC	*International Electrotechnical Commission*
NIST (USA)	*National Institute for Standards and Technology*

U oblasti bezbednosti informacija, ISO/IEC su objavili najviše standarda od kojih je najznačajnija tzv. serija ISO/IEC 27000, koja dosta liči na seriju standarda ISO 9000 za kontrolu kvaliteta.

U oblasti bezbednosti informacija, ISO/EC su objavili najviše standarda od kojih je najznačajnija tzv. serija ISO/IEC 27000, koja dosta liči na seriju standarda ISO 9000 za kontrolu kvaliteta (**Prilog 1**).

Standarde zaštite informacija donosi *Međunarodni tehnički komitet za standardizaciju ISO/IEC JTC1/SC27***,** formiran 1990. (Sl. 2.2) [61].



Sl. 2.2. Organizaciona šema Tehničkog komiteta ISO/IEC JTC 1SC 27

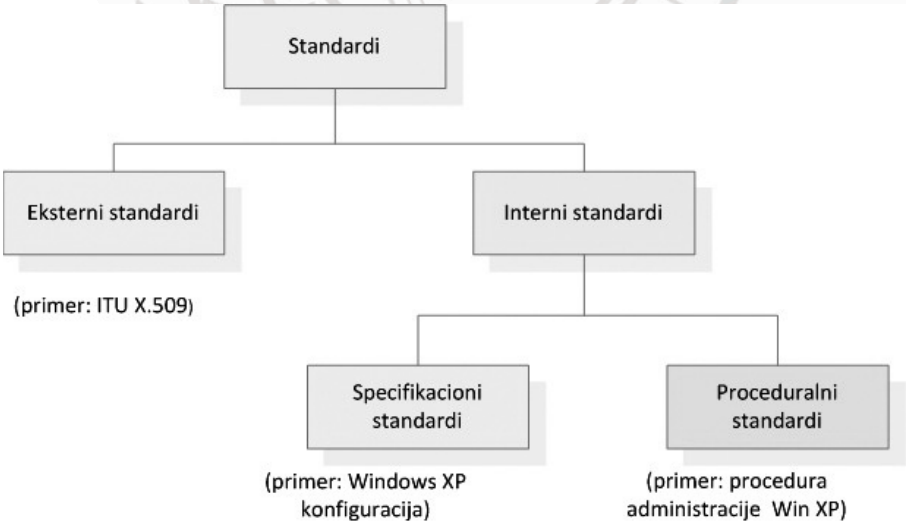
Obim poslova Komiteta su standardi za zaštitu informacija i IKTS, uključujući generičke metode, tehnike i uputstva, koji obuhvataju sve aspekte zaštite informacija i privatnosti, kao što su: *metodologija za upravljanje bezbednosnim zahtevima; ISMS; kriptografski i drugi mehanizmi zaštite; dokumentacija i terminologija zaštite; bezbednosni aspekti upravljanja identitetom i zaštitom privatnosti; metodologija i kriterijumi za evaluaciju zaštite* itd.

Komitet ima pet radnih grupa: **WG1 –** za upravljanje zaštitom, **WG2** – za kriptografske algoritme i druge mehanizme zaštite, **WG3 –** kriterijumi za procenu/evaluaciju zaštite, **WG4** – servisi i kontrole zaštite i **WG5** – tehnologije za zaštitu privatnosti i upravljanje identitetom [12, 22, 24, 25, 26].

2.4. 4. Klasifikacija standarda zaštite

Uobičajena klasifikacija standarda zaštite je na *eksterne i interne*.

Eksterni (industrijski) standardi, tzv. *standardi najbolje prakse zaštite* su šire prihvaćeni i namenjeni (ali ne isključivo) za *upravljanje sistemom zaštite, analizu rizika, obuku, evaluaciju i sertifikaciju i akreditaciju sistema i proizvoda zaštite*. Prednosti u odnosu na interne standarde su u tome što obezbeđuju bolje testiranje proizvoda zaštite, lakše otkrivanje i brže fiksiranje ranjivosti i bržu razmenu iskustva iz prakse zaštite. Nedostaci su što ih periodično treba usaglašavati sa kriterijumima za razvoj sistema zaštite (Sl. 2.3.) [74].



Sl. 2.3 Klasifikacija standarda zaštite

Eksterni standardi su najčešće korišćeni u praksi zaštite i obuhvataju set širom sveta, empirijski potvrđenih principa zaštite [*43, 48, 49, 50, 64*]. *Definicija* najbolje prakse zaštite informacija je kompleksna, raznolika i obuhvata više izvora. Na *meta* nivou definiše se kao: *„Dokumentovane, pristupačne, efikasne, odgovarajuće i široko prihvaćene strategije, planovi, taktike, procesi, metodologije, aktivnosti i pristupi, razvijeni od strane kompetentnih entiteta i izvršeni sa adekvatno obučenim personalom, koji su usklađeni sa postojećim zakonima i regulativama, vremenom se potvrdili kroz istraživanje, evaluaciju i praksu kao efektivni u obezbeđivanju zaštite na prihvatljivom nivou rizika i koji se neprekidno revidiraju i poboljšavaju u skladu sa promenama okruženja, tehnologija, pretnji, organizacije i sl.*" [61]. Ovaj pristup („*odozgo nadole*") pomaže u razumevanju osnovnih i ključnih atributa generičke, najbolje prakse i elemenata, važnih za zaštitu informacija [21, 74].

Glavni ciljevi ovih standarda su da *promovišu najbolju praksu* zaštite, *poboljšaju nivo bezbednosti*, *smanje rizik* na prihvatljiv nivo i pomognu *dalji razvoj* standarda. Za uspostavljanje upravljivog poslovnog okruženja, gde se rizik mora držati pod kontrolom, potrebno je, na bazi procene rizika, *redefinisati kontrole* najbolje prakse zaštite i izabrati one koje daju najbolje rezultate, *implementirati standard u sve faze životnog ciklusa* i *upravljati promenama* – održavati efektivan i efikasan skup kontrola zaštite na bazi regularne procene rizika. Implementacija standarda najbolje prakse zaštite pomaže organizaciji: *da se uključi u međunarodno prihvaćenu praksu zaštite, upravlja rizikom, izgradi poverenje drugih entiteta, smanji štetne posledice glavnih incidenata, uspešno bori protiv kompjuterskog kriminala, usklađuje praksu sa pravnim i normativnim zahtevima, održava kontinuitet poslovanja* i dr. Najbolja praksa zaštite tipično se implementira u program IKTS zaštite uz podršku i aktivnu saradnju *menadžmenta*, *administratora sistema, administratora i tehničkog revizora zaštite* [21, 43].

Glavni nedostatak je ne postojanje *jedinstvenog modela najbolje prakse zaštite.* Razlozi su brojni faktori, kao što su različiti uticaji nacionalnih zakona i pravnih okvira u drugim zemljama, različitih i brojnih definicija najbolje prakse, veliki broj sertifikacionih tela i dr. Do sada najpotpuniji model najbolje prakse zaštite nalazi se u priručniku „*Hierarchy of Security*" [64].

Interni standardi uključuju *specifikacione* i *proceduralne* standarde. *Specifikacioni* standardi definišu osnovnu zaštitu za datu konfiguraciju IKTS, na bazi teorije zaštite i izbora kontrola osnovne zaštite (*security baseline*) iz kataloga *kontrola za najbolju praksu zaštite*. Za izradu ovakvog standarda za veći, visoko distribuirani IKTS u Internet okruženju, potrebno je oko šest meseci rada. K*ontrole osnovne zaštite* moraju se u fazi razvoja i implementacije dopuniti na bazi analize i procene rizika sa kontrolama zaštite, specifičnim za sistem i okruženje. *Proceduralni interni standardi* (upravljačke i organizaciono-operativne kontrole) su korisni mehanizmi za opisivanje procedura procesa za administraciju i organizaciju prakse zaštite i uključuju samo važne korake bez tehničkih detalja. Uglavnom su generički i nisu specifični za platformu računarskog sistema. Tehnički detalji se opisuju u tehničkoj dokumentaciji za uređaje/sisteme zaštite.

2.4.5. Prednosti i nedostaci standarda zaštite

Osnovne prednosti standardizacije zaštite IKTS su [1,6,12, 27, 43]:

- *smanjenje kompleksnosti* upravljanja sistemom zaštite,
- veća mogućnost izbora i izrada *standardne dokumentacije,*
- obezbeđenje *interoperabilnosti* različitih sistema zaštite,
- formiranje *baze znanja* iz oblasti zaštite,
- nezamenljivi alat u procesima sertifikacije i akreditacije sistema zaštite,
- obezbeđuje osetljive metode i definiše najbolju praksu zaštite.

Osnovni nedostatak standardizacije zaštite je što ne postoji integralni standard za upravljanje zaštitom, tipa opšte prihvaćenog standarda za upravljanje sistemom zaštite (ISMS standard ISO/IEC 27001), koji bi pored odgovora „**ŠTA"** dao instrukcije i „**KAKO"** to treba uraditi u zaštiti (tipa ISO/IEC 21827 ili SSE CMM – *System Security Engeneering Capability Maturity Model,* rev. 2008) [49]. Međutim, zbog prirode koncepta zaštite, verovatno je dobro da se takvi standardi nikada ne pojave.

Implementacija standarda i normativno usklađivanje, sami po sebi nisu dovoljni. Ako su konzistentno primenjeni, standardi obezbeđuju optimalne uslove za razvoj programa i projektovanje sistema zaštite, a normativno usklađivanje obezbeđuje zaštitu specifičnih i osetljivih informacija. U programu zaštite preporučuje se integracija internih i eksternih standarda najbolje prakse zaštite i usaglašavanje sa normativima, da bi se izgradio sveobuhvatni okvir za merenje i evaluaciju procesa zaštite u organizaciji. Lista relevantnih standarda zaštite data je u **Prilogu 2.**

2.5. NORMATIVNI OKVIR ZAŠTITE

Normativni okvir obezbeđuje značajne funkcije osnovnog sloja zaštite, kao što su: ističe značaj zaštite informacija na državnom nivou, koncentriše resurse na strateškim pravcima istraživanja i razvoja, zahteva obuku i obrazovanje, sankcioniše zloupotrebe zaštite, obavezuje na sertifikaciju i akreditaciju i dr. U normativnom okviru posebno mesto imaju podzakonski pravni akti (npr. Pravilnici o uspostavljanju PKI (Public Key Infrastructure), CA i digitalnog potpisa itd.) i standardi zaštite [37, 58, 77].

Na nivou svake države uglavnom postoji Zakon o zaštiti informacija, koji obavezuje pojedince i poslovne sisteme da štite svoje informacije u e-okruženju, propisuju obavezan obim zaštite, od čega i kako štititi privatnost korisnika i kakve su sankcije za povrede sistema zaštite [75, 76]. Pored zakona o zaštiti informacija, na nivou države potrebni su i donose se brojni zakoni koji regulišu kompjuterski kriminal (Zakon o kompjuterskom kriminalu, Zakon o digitalnom dokazu, Zakon o sudskom veštačenju u oblasti IKT, Zakon o formiranju CIRT i CERT tela i dr.) [13, 32].

Globalni karakter kompjuterskog kriminala zahteva da se u razvoju programa zaštite razmatraju *usklađenost sa međunarodnim zakonima, regulativama i standardima*, *razlike pravosudnih sistema*, *ugovorne i obaveze o čuvanju poslovnih tajni, zaštita privatnosti i ličnih podataka*.

U razvoj programa zaštite treba uključiti nacionalni zakonski okvir, koji reguliše tip podataka kojima se pristupa, načine korišćenja, skladištenja ili procesiranja u IKTS organizacije i identifikovati sve primenljive normativne zahteve. Globalizacija IKT i transnacionalna priroda kompjuterskog kriminala, zahtevaju *usklađenost zakona, regulativa i standarda zaštite* na međunarodnom nivou. *Razlike u pravosudnim sistemima* utiču na istragu transnacionalnog kompjuterskog kriminala. Takođe, legalni zahtevi državnih organa za zadržavanje podataka, kao i za zaštitu privatnosti u periodu njihovog zadržavanja, variraju od države do države. EU je usvojila *Direktivu o privatnosti i elektronskim komunikacijama* (25.07.2002.), zahtevajući od provajdera Internet servisa da u određenom periodu zadržavaju podatke na svim e-komunikacijama. Autorska prava moraju biti zaštićena na način koji zadovoljava legalne zahteve. *Poverljive i informacije o intelektualnoj svojini,* program zaštite mora štititi na način koji zadovoljava minimalne zahteve zakona o zaštiti poverljivih informacija, da bi se moglo obezbediti zakonsko gonjenje počinioca u pravosudnom sistemu gde je krivično delo izvršeno.

U mnogim zemljama *Zakon o borbi protiv kompjuterskog kriminala* je neadekvatan i ne pokriva na isti način transnacionalni kriminal, koji se mora istraživati, dokazivati i sankcionisati usaglašenim i standardizovanim procedurama i alatima u svim uključenim pravosudnim sistemima [1].

Ugovori i ugovori o neotkrivanju poslovnih tajni – NDA *(Non Disclose Agreement)* moraju na isti način tretirati vlastite i IKTS objekte druge ugovorne strane, što često nije slučaj. Organizacije moraju imati eksplicitnu politiku i procedure zaštite koje zadovoljavaju zahteve zakona o kompjuterskom kriminalu i neotkrivanju poslovnih tajni u konkretnom pravosudnom sistemu.

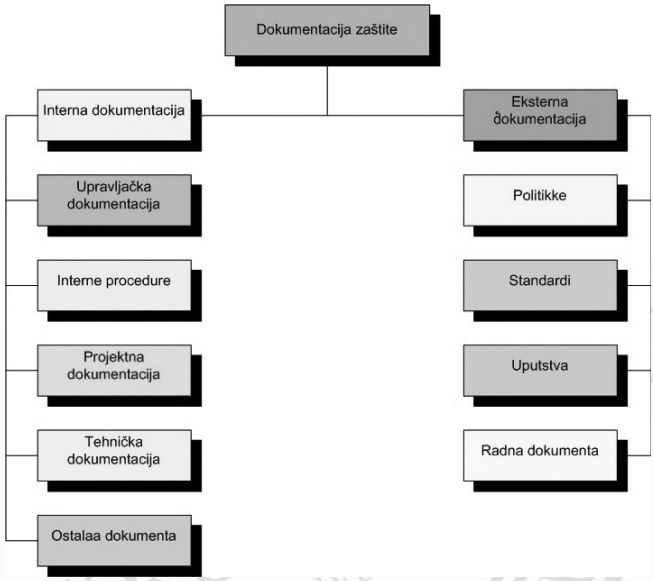
Zaštita privatnosti i ličnih podataka u brojnim pravosudnim sistemima, nije kompletirana i usaglašena sa zakonima EU, uprkos velikom pritisku javnosti. Preporuke da se privatnost i lični podaci štite opštim i tehničkim merama zaštite, ostavljaju prostor za proizvoljnost i uvek su jeftinije rešenje za organizaciju, nego obavezna zaštita propisana zakonom.

2.6. DOKUMENTACIJA ZAŠTITE

U OOM metodološka osnova programa zaštite je dokumentacija zaštite, koja se može klasifikovati ma internu i eksternu. Osnovni zahtevi za dobru dokumentaciju zaštite su da bude *laka za upotrebu/održavanje,* da *sadrži tačne i ažurne informacije, da je odgovarajuća za ciljne korisnike i da sadrži samo relevantne i bitne informacije.*

Bezbednost i zaštita informacija nisu statički elementi. Od kritičnog značaja je da se revizija dokumenata zaštite vrši najmanje jedanput godišnje, a za operativnu zonu, koja zahteva veći stepen zaštite, i češće. Revizija uključuje dokumenta zaštite, korekciju otkrivenih ranjivosti, usaglašavanje sa promenama standarda, normativa, tehnologija i okruženja, a često i ažuriranje politike i procedura zaštite.

Glavne kategorije dokumentacije zaštite prikazane su na slici 2.4. [74]



Sl. 2.4. Klasifikacija dokumentacije zaštite

Primeri dokumentacije zaštite prikazani su u tabeli 2.3.

Tabela 2.3. Primeri dokumentacije zaštite

Interna dokumentacija	
Upravljačka dokumentacija	ugovori, planovi, izveštaji, NDA itd.
Interne procedure	za izveštavanje, reviziju izmena, administraciju itd.
Projektna dokumentacija	za implementaciju skenera zaštite itd.
Tehnička dokumentacija	uređaja zaštite, tehnički izveštaji, testovi i sl.
Ostala dokumenta	materijal za obuku, dokumenta sa konferencija itd.
Eksternu dokumentaciju	
Program zaštite	programsku politiku na nivou organizacije
ISMS politika	za upravljanje sistemom zaštite informacija
Industrijski standardi	za upravljanje, obuku, nadzor i reviziju itd.
Uputstva za zaštitu	za upravljanje VD, administraciju zaštite itd.
Radna dokumenta	radne liste, uzorci, katalozi kontrola zaštite i dr.

Uputstva zaštite ne uvode promene u upravljački okvir, za razliku od standarda zaštite. Čine ih *upravljačka* i *tehnička uputstva,* koja daju detaljnije informacije o specifičnim pitanjima zaštite. *Radna dokumenta* su namenjena za povećavanje razumevanja prakse zaštite (grafičke prezentacije i ček liste, tehnički bilteni itd.).

2.7. REZIME

Konzistentni principi zaštite informacija su osnovni, gradivni elementi na kojima se zasnivaju procesi zaštite. *Opšte prihvaćeni principi zaštite* (*GAISP)* usmeravaju menadžment na izvršnom nivou i pomažu organizaciji da definiše efektivnu strategiju zaštite. Namenjeni za upravljanje sistemom zaštite, fundamentalni su i retko se menjaju. GAISP principi obuhvataju tri kategorije - *opšte, funkcionalne i detaljne pri*ncipe. *Opšti GAISP principi* se odnose na upravljanje i sadrže devet principa. *Funkcionalni* su gradivni blokovi opštih, a odnose se na operativno upravljanje i detaljnije definišu taktiku izgradnje efektivne arhitekture sistema zaštite. *Detaljni GAISP principi* zaštite koriste funkcionalne kao okvir, namenjeni su za profesionalce, a obezbeđuju specifično, sveobuhvatno uputstvo za dnevne aktivnosti u procesu upravljanja rizikom i sistemom zaštite.

Standardi zaštite obezbeđuju pravila za upravljanje sistemom zaštite, a mogu se izvoditi iz normativa, industrijske prakse ili iskustava. Primarni cilj standarda nije sama standardizacija, nego *smanjenje kompleksnosti sistema upravljanja zaštitom, mogućnost izbora standardne dokumentacije i obezbeđenje interoperabilnosti*.

Eksterni industrijski standardi su brojni, na primer za upravljanje sistemom zaštite, analizu rizika, obuku itd. *Interni standardi,* specifični za organizaciju, predstavljaju jezgro za formiranje okvira za upravljanje, dodaju vrednost poslovanju i pomažu interpretaciju politike zaštite. Dele se na *specifikacione* i *proceduralne*. S*tandardi najbolje prakse zaštite* obezbeđuju kontrole za osnovnu zaštitu. Za specifičnu organizaciju i okruženje, ove kontrole je potrebno ažurirati na bazi procene rizika.

Normativni okvir obezbeđuje pravni okvir i obavezu organizovanja i uspostavljanja sistema zaštite informacija i sankcionisanja prekršioca; ističe značaj problematike zaštite na najvišem državnom nivou; koncentriše resurse na najznačajnijim, strateškim pravcima istraživanja; koordinira obuku i obrazovanje; obavezuje sertifikaciju i akreditaciju sistema zaštite i dr.

Metodološku osnovu programa zaštite čine *interna* i *eksterna* dokumentacija. *Interna dokumentacija,* u odnosu na sistem zaštite, obuhvata *upravljačku dokumentaciju, procedure, projektnu i tehničku dokumentaciju i ostala dokumenta*. *Eksterna dokumentacija* obuhvata *politiku zaštite, industrijske standarde, uputstva za zaštitu* i druga *radna dokumenta*. *Uputstva za zaštitu* su precizne instrukcije za upravljanje sistemom zaštite, koje ne obavezuju korisnike da ih striktno sprovode za razliku od zakona i standarda zaštite.

2.8. KLJUČNI TERMINI

Detaljni GAISP principi zaštite: gradivni blokovi funkcionalnih principa, obezbeđuju specifična, sveobuhvatna uputstva za dnevne aktivnosti u procesima upravljanja zaštitom.

Eksterni standardi zaštite: nastaju izvan organizacije koja ih koristi, šire su prihvaćeni za upravljanje sistemom zaštite i druge procese zaštite.

Funkcionalni GAISP principi zaštite: detaljnije definišu taktiku izgradnje efektivne arhitekture sistema zaštite i čine gradivne blokove opštih principa.

GAISP principi zaštite: sveobuhvatna hijerarhija instrukcija za obezbeđenje opšte prihvaćenog, konzistentnog okvira za zaštitu informacija, koji mogu imati i izuzetke.

Interni standardi zaštite: specifični su za organizaciju i dele se na specifikacione i proceduralne; jezgro su za upravljanje sistemom zaštite i dodaju vrednost IKTS.

Normativni okvir: zakoni i podzakonska akta u oblasti zaštite obezbeđuju osnovni okvir za širu implementaciju programa zaštite IKTS i mehanizme sankcionisanja za nesprovođenje.

Opšti GAISP principi: namenjeni za upravljanje sistemom zaštite, fundamentalni su, retko se menjaju, a obuhvataju 9 principa za zaštitu informacija.

Princip: fundamentalna istina, ili zakonitost koja se uzima bez dokazivanja kao osnova za izvršavanje racionalne aktivnosti u procesu realizacije nekog koncepta.

Proceduralni interni standardi: mehanizmi za opisivanje procedura za administratore ili korisnike zaštite; uključuju samo najvažnije korake, bez tehničkih detalja i generički su.

Specifikacioni interni standardi: definišu optimalan sistem osnovne zaštite za datu konfiguraciju IKTS.

Standardi zaštite: obezbeđuju pravila upravljanja sistemom zaštite, a mogu se izvoditi iz normativa, industrijske prakse i iskustava.

2.9. PITANJA ZA PONAVLJANJE

1. Skup *sistemskih* principa zaštite predstavlja obavezan okvir u koga se ugrađuju specifični GAISP principi zaštite, a obuhvata:
   a. nikad sam, rotacija radnih mesta, razdvajanje dužnosti, minimum privilegija
   b. nikad sam, rotacija radnih mesta, razdvajanje dužnosti, minimum privilegija, znati samo što je potrebno, principe upravljanja IKT sistemom
   c. uvek sam, rotacija radnih mesta, razdvajanje dužnosti, znati samo što je potrebno, minimum privilegija, principe upravljanja IKT sistemom
   d. što duže na jednom radnom mestu, objediniti što više dužnosti radi smanjenja kadrova, upravljanje zaštitom razdvojiti od upravljanja IKT sistemom
2. Isto lice ne može istovremeno obavljati sledeće parove funkcija u IKTS:
   a. operativni rad na računaru – programiranje
   b. unos i priprema podataka za obradu – čuvanje elektronskih medija;
   c. obrada podataka – kontrola kvaliteta IKTS
   d. operativni rad na računaru – obrada podataka
   e. prijem osetljivih informacija – predaja osetljivih informacija
   f. programiranje aplikacija – kontrola ovlašćenja za pristup
   g. programiranje aplikacija – administracija baza podataka
   h. projektovanje, implementacije/modifikacija sistema zaštite – programiranje

3. Princip minimuma privilegija znači:
   a. davati minimum pristupa objektima IKTS
   b. davati što je moguće manje privilegovanih prava pristupa objektima IKTS
   c. davati pristup što manjem broju korisnika objektima IKTS
4. Sistemski princip *nikad sam*:
   a. sprečava monopolski položaj
   b. sprečava samokontrolu u IKTS i sistemu zaštite
   c. obezbeđuje samokontrolu u IKTS i sistemu zaštite
   d. zahteva zapošljavanje najmanje dva lica na bezbednosno relevantno mesto
   e. znači da ni jedan servis zaštite ne treba da kontroliše samo jedan administrator zaštite
5. O*pšte prihvaćene principe zaštite* (GAISP) mogu da koriste:
   a. specijalisti zaštite za razvoj sistema zaštite
   b. proizvođači u proizvodnji komponenti i uređaja zaštite
   c. menadžeri za razvoj i implementaciju poslovnih procesa
   d. proizvođači proizvoda zaštite u procesu prodaje komponenti/uređaja zaštite
   e. vlasnici informacija i menadžeri za razvoj programa zaštite
6. Navedite koji principi spadaju u opšte GAISP principe zaštite:
   a. princip svesti o potrebi zaštite i odgovornosti
   b. princip stalnog preispitivanja i etičkog ponašanja
   c. princip povremenog preispitivanja i procene
   d. princip proporcionalnosti i dekompozicije
   e. princip multidisciplinarnosti i dezintegracije
7. Princip proporcionalnosti znači da:
   a. kontrole zaštite treba projektovati, implementirati i primenjivati za zaštitu informacija proporcionalno proceni rizika
   b. kontrole zaštite treba projektovati, implementirati i primenjivati za zaštitu informacija proporcionalno zahtevima korisnika
   c. sistem zaštite treba projektovati, implementirati i primenjivati za zaštitu informacija proporcionalno zahtevu vlasnika sistema
8 Detaljni principi zaštite namenjeni su:
   a. vlasnicima sistema
   b. izvršnim menadžerima
   c. specijalistima zaštite
9. Primarni cilj standarda zaštite je*:*
   a. sama standardizacija zaštite
   b. smanjenje kompleksnosti zaštite
   c. mogućnost izbora i izrade standardne dokumentacije
   d. obezbeđenje interoperabilnosti sistema zaštite
   e. formiranje baze znanja iz oblasti zaštite
10. Glavni ciljevi standarda najbolje prakse zaštite su:
   a. promovisanje najbolje prakse zaštite
   b. smanjenje nivoa bezbednosti
   c. smanjenje rizika na prihvatljiv nivo
   d. omogućavanje daljeg razvoja mehanizam zaštite
11. Standard zaštite:
   a. je usvojen i objavljen dokument
   b. uspostavlja specifikaciju i procedure
   c. obezbeđuje da dokumenta, materijali, proizvodi, metodi ili servisi zaštite, odgovaraju nameni i konzistentno izvršavaju saopštenja politike zaštite
   d. sadrži skup rešenja za pokrivanje specifičnih bezbednosnih zahteva za održavanje rizika na prihvatljivom nivou
   e. obezbeđuje instrukcije za razvoj, implementaciju i održavanje IKTS
   f. uvodi promene u upravljački okvir sistema zaštite
12. Standard ISO/IEC 27001 obezbeđuje:
   a. uputstvo za upravljanje i izbor kontrola zaštite
   b. standard za upravljanje sistemom zaštite informacija

c. upravljačke, operativne i tehničke kontrola zaštite
d. tehnički standard za specifične tehnologije i metriku za evaluaciju zaštite

13. Generički, hijerarhijski model standarda zaštite uključuje:
    a. principe, metodologiju, elemente standarda, uputstvo, dodatke za primenu, tehnike i alate
    b. terminologiju, elemente standarda, uputstvo, dodatke za primenu, tehnike i alate
    c. terminologiju, principe, metodologiju, elemente standarda, uputstvo, dodatke za primenu, tehnike i alate
    d. terminologiju, principe, metodologiju, elemente standarda, tehnike i alate
14. Standarde zaštite informacija donosi tehnički komitet:
    a. BSI
    b. BSI (GERMAN)
    c. ISO/IEC JTC1/SC27
    d. NIST (USA)
    e. ISO
15. Standardi zaštite se klasifikuju na:
    a. eksterne i interne
    b. industrijske i organizacijske
    c. specifikacione i proceduralne
    d. tehničke i proceduralne
16. Osnovne karakteristike dobre dokumentacije zaštite su:
    a. laka za upotrebu/održavanje i sadrži tačne i ažurne informacije
    b. što kraća i sa glavnim podacima, odgovarajuća za sve korisnike
    c. sadrži opšte podatke iz vremena izrade dokumentacije
    d. odgovarajuća za sve grupe korisnika, sadrži samo relevantne informacije
    e. odgovarajuća za ciljne korisnike i sadrži samo relevantne i bitne informacije
17. Interna dokumentacija zaštite uključuje:
    a. upravljačku dokumentaciju i interne procedure
    b. program zaštite i ostalu dokumentaciju (materijal za obuku, instrukcije)
    c. politiku zaštite i industrijske standarde
    d. projektnu dokumentaciju i tehničku dokumentaciju
    e. uputstva za zaštitu i radna dokumenta (kontrolne liste, uzorci, katalozi, ...)
18. Eksterna dokumenta zaštite uključuju:
    a. upravljačku dokumentaciju i interne procedure
    b. program zaštite i ostalu dokumentaciju (materijal za obuku, instrukcije)
    c. ISMS politiku zaštite i industrijske standarde
    d. projektnu dokumentaciju i tehničku dokumentaciju
    e. uputstva za zaštitu i radna dokumenta (kontrolne liste, uzorci, katalozi...)
19. Osnovne funkcije normativa zaštite informacija su:
    a. ističe značaj zaštite informacija na nivou organizacije
    b. koncentriše resurse na taktičkom nivou istraživanja i razvoja
    c. zahteva obuku i obrazovanje, sankcioniše zloupotrebe
    d. obavezuje na sertifikaciju i akreditaciju
20. Glavni atributi kvaliteta standarda zaštite su:
    a. dokumentovan, raspoloživ i sveobuhvatan
    b. izdat od strane nacionalnog tela za standardizaciju
    c. adekvatan nameni, rentabilan, obavezno prihvaćen
    d. usaglašen sa zakonima i da obezbeđuje indikatore progresa
    e. usaglašen sa politikom zaštite i da obezbeđuje indikatore progresa

3. METODOLOGIJE, MODELI I OKVIRI SISTEMA ZAŠTITE

Po završetku ovog poglavlja razumećete:

- značaj metodologije i okvira za razvoj sistema zaštite
- opštu metodologiju za razvoj programa i sistema zaštite
- značaj modelovanja procesa, komponenti i sistema zaštite
- strukturni i objektno orijentisani model sistema zaštite

3.1. UVOD

Metodologije i okviri zaštite IKTS uspostavljaju se u kontekstu organizacije na osnovu internih ili šire prihvaćenih industrijskih standarda. Metodologije i okviri se grupišu zajedno, najčešće kao *upravljačke kontrole* i dodaju strukturu procesima zaštite.

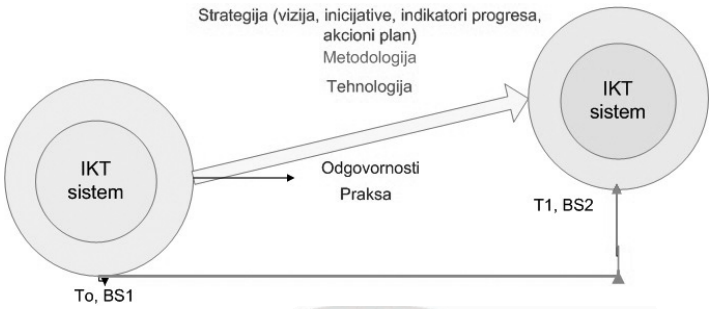
Za razvoj i implementaciju sistema zaštite ključni koncepti su *metodologija, tehnologija, praksa* i *odgovornosti* u zaštiti. Klasična metodologija za razvoj životnog ciklusa IKTS – ***SDLC*** (*System Development Life Cycle*) preuzeta je kao formalna metodologija i za razvoj sistema zaštite [59]. Međutim, ova ni bilo koja standardna metodologija, nisu pogodne za većinu razvojnih projekata savremenih IKTS (npr. za e-poslovanje i podsisteme zaštite), koji se razlikuju od klasičnih po distribuciji servisa, brzini promena okruženja i tehnologija, pa zahtevaju nove pristupe procesima projektovanja i razvoja. U praksi zaštite malo je verovatno da će se primenjena metodologija podudariti sa bilo kojom poznatom. Obično projektant izabere metodologiju koja najviše odgovara, a zatim *kreira sopstvenu*, kombinujući poznate metodologije.

Metodologije za razvoj tradicionalnih IKTS (*SDLC*, *vodopada, brzog odziva* itd.), razvijane su za različita okruženja i ne mogu se lako preneti u *web* okruženje sa enormnim porastom rizika. Za zaštitu *web* aplikacija od presudnog značaja je pouzdano upravljanje *kvalitetom* sistema zaštite *web* aplikacija gde je primenljiva, na primer, *metodologija vektora zaštite*, koja kombinuje standarde *ISO/IEC 15408, ISO/IEC 27001 i ISO/IEC 21827* [45, 50, 49].

3.2. METODOLOŠKI OKVIRI ZA RAZVOJ SISTEMA ZAŠTITE

Dugoročni okvir za razvoj sistema zaštite obezbeđuje *strategija zaštite*. Koncept strategije zaštite uključuje *presek stanja sistema zaštite, viziju željenog bezbednosnog*

stanja, inicijative za dostizanje tog stanja, sistem indikatora za praćenje progresa i akcioni plan za izvršavanje strateškog cilja (Sl. 3.1).



Sl. 3.1. Strategija bezbednosti IKTS u funkciji sistema zaštite

Razvoj i implementacija sistema zaštite obuhvata četiri ključna koncepta: *metodologiju*, *tehnologiju*, *operativnu praksu i odgovornosti* (Tabela 3.1).

Tabela 3.1. Ključni koncepti za razvoj sistema zaštite

Koncepti	Primeri realizacije
Metodologija	*Principi*: GAISP (sveobuhvatnost, integralnost, modularnost ...). *Modeli*: IKTS, procesa, arhitekture sistema zaštite itd. *Metodi:* kvantitativni, kvalitativni; primena standarda najbolje prakse. *Razvoj procesa:* projektno–procesni i SE pristup; plan zaštite …
Tehnologija	*Alati i tehnike*: hardversko–softverski; manuelne, polu-automatske tehnike. *Tehničke kontrole:* hardversko/softverski mehanizmi i protokoli.
Praksa zaštite	*Operativne kontrole*: aktivnosti proceduralne zaštite.
Odgovornost	*Upravljačke kontrole*: pripisivanje odgovornosti za zaštitu.

Metodologije i okviri u oblasti zaštite razvijaju se na bazi internih i/ili opšte prihvaćenih industrijskih standarda. Oba konteksta su jednako značajna. Primeri metodologija i okvira zaštite su brojni [44, 49, 63, 74].

Kada neka organizacija primeni metodološki okvir na određeni projekat zaštite, razmatrajući sve organizacione, projektne i timske varijable, malo je verovatno da će se okvir potpuno podudariti sa bilo kojom poznatom metodologijom za razvoj IKTS. Savremeni IKTS za e-poslovanje, *web* servise u *distribuiranom Internet računarstvu* – **CC** (*Cloud Computing*) i sistemi njihove zaštite, zahtevaju veću pažnju za razvoj interfejsa čovek–mašina za automatizaciju upravljanja, veću potrebu za timskim radom i nove pristupe procesima projektovanja i razvoja.

Svaka metodologija u potpunosti je određena definisanjem: *principa, koncepata*, *metoda* i *toka razvoja procesa zaštite***.** *Principi* su aksiomatske, fundamentalne istine, ili relativno nepromenljive zakonitosti koje se uzimaju kao osnova za izvršavanje racionalne aktivnosti u procesu realizacije nekog koncepta. U oblasti zaštite usvojeni su GAISP principi. *Koncept zaštite*, najčešće model, približna je aproksimacija realnog sistema zaštite, kojim se definiše razumevanje osnovnih *funkcionalnosti* ili *strukturnih* elemenata organizacije zaštite. U praksi zaštite, najčešće upotrebljavani modeli su *funkcionalni, strukturni i objektno–orijentisani*, a koncepti – *reaktivnog i proaktivnog* sistema zaštite. Detaljan pregled primenljivih modela u oblasti zaštite, može se naći u literaturi [6, 10, 25, 34].

U razvoju sistema zaštite generalno se koriste tri moguće metodologije, koje kao upravljački okvir koriste [74]: (1) *politiku zaštite,* (2) *procenu rizika, (3) standarde najbolje prakse zaštite* i njihove kombinacije. Primenjene pojedinačno, ove metodologije obezbeđuju koncept klasičnog, *reaktivnog sistema zaštite*, ili zaštite od *poznatih* napada. Kombinovane, namenjene za najviši nivo (idealne) zaštite i univerzalne tipove organizacija, poslovnog okruženja i profila rizika, obezbeđuju zaštitu od *poznatih* i *nepoznatih* pretnji (tzv. *proaktivnu zaštitu*). Metodologija na bazi standarda najbolje prakse zaštite ne uzima u obzir realno stanje konkretne organizacije, pa za jednu organizaciju može biti idealna, a za drugu redundantna ili ne-efektivna. Ova metodologija daje dobre rezultate u kombinaciji sa ažurnom politikom zaštite i regularnom procenom rizika, koja obezbeđuje neophodne konkretne informacije za *optimalnu zaštitu*.

Tehnologije zaštite (*tehnike i alati)* su hardversko softverski mehanizmi i protokoli implementirani u sistem zaštite. Pod *alatima zaštite* se u širem smislu podrazumevaju *proceduralne (upravljačke i operativne)* i *tehničke kontrole* (hardversko-softverski mehanizmi i protokoli) zaštite. Alati su sredstva za realizaciju koncepata zaštite, a metodi primene alata uključuju *tehnike zaštite*, koje su dokumentovane obično u tehničkoj dokumentaciji uređaja za zaštitu**.**

Procesni razvoj sistema zaštite zahteva poznavanje, planiranje, formalni opis, definisanje, kontrolu, evaluaciju i poboljšavanje *procesa zaštite*. U metodologiji sistemskog inženjerstva (*SE) proces* je skup ljudi, sredstava i povezanih aktivnosti, usmerenih za postizanje nekog jedinstvenog cilja; proces ima svoj početak i kraj, a u kontekstu sistema zaštite može se ciklično neprekidno ponavljati (npr. nadzor i revizija, obuka i edukacija). Redosled izvršavanja aktivnosti u procesu zaštite definišu *procedure zaštite,* koje dokumentuju procese zaštite**.** Proces zaštite je i *transformator* ulaznih veličina u sistem zaštite u, očekivano, veće izlazne veličine i *integrator* ključnih atributa posla: ljudi, tehnologija i metoda za izvršavanje zadataka [86].

Projekat zaštite uključuje proces/skup procesa usmerenih na izvršavanje zajedničkih zadataka i postizanje jedinstvenog bezbednosnog cilja, ograničene resurse za realizaciju (tim, vreme, sredstva) i njihove međusobne veze. Zbog kompleksnosti savremenih IKTS, strateške inicijative zaštite retko se implementiraju kroz jedan projekat. Obično se razvoj sistema zaštite razbija na manje projekte, koji se mogu izvršiti za tri do šest meseci, sa

relativno manjim budžetom i koji se implementiraju prema prioritetima utvrđenim na bazi bezbednosnih zahteva i procene rizika [74].

3.3. MODELOVANJE SISTEMA ZAŠTITE

3.3.1. Strukturni modeli distribuiranog IKT sistema

Model je apstrakcija realnog sistema, a koristi se za pojednostavljenu prezentaciju problema kojeg treba rešiti. Postoje četiri generička tipa modela: *fizički* (npr. automobila), *narativni* (npr. pisani i tekstualni), *grafički* (*npr.* arhitektura sistema) *i matematički* (formalni za kritične i skupe procese). U modelovanju IKTS i sistema zaštite koriste se *narativni* (najčešće *funkcionalni*), *grafički i matematički* modeli. Namena svakog modelovanja je da smanji kompleksnost sistema. U modelovanju sistema zaštite preuzeti su i koriste se svi klasični modeli za modelovanje IKTS: *linearni (životnog ciklusa, vodopada), iterativni, sa brzim odzivom* itd. Zbog kompleksnosti IKTS i sistema zaštite, u projektovanju i razvoju sistema zaštite najbolje rezultate pokazuju *strukturni* i *objektno orijentisani* modeli (OOM).

Strukturni model zaštićenog (bezbednog) IKTS sadrži tri glavne komponente: (1) skup pasivnih i aktivnih *objekata,* kojima se pristupa na kontrolisan način, (2) skup aktivnih *subjekata*, koji koriste i pristupaju objektima i (3) skup *pravila* na osnovu kojih subjekti koriste i pristupaju objektima. Strukturni modeli koriste princip *dekompozicije* objekata IKTS na skupove, prema definisanim kriterijumima (jedinstveni bezbednosni ciljevi, jedinstvene funkcije itd.), a odbacuju nebitne komponente i tako smanjuju kompleksnost sistema. U sledećim primerima dati su neki tipovi primene *strukturnih modela* [81].

Primer 1: Strukturni model visoko distribuiranih zaštićenih IKTS OSI modela, obuhvata sledeće *bezbednosno relevantne grupe dekomponovanih objekata*, koji se, sa svoje strane, mogu po potrebi dalje dekomponovati na: *lokalnu mrežu, kanale i sredstva veze, komutacione uređaje, centar za obradu informacija, udaljene pristupe, legalne i nelegalne korisnike sistema, nosioce informacija (magnetne, optičke i dr.), izdvojene radne stanice i tehniku bekapovanja* [21].

Primer 2: U modelovanju mehanizma logičke kontrole pristupa, u određenom vremenskom trenutku svi tipovi korišćenja i pristupa subjekata (**S**) objektima sistema (**O**) čine bezbedno stanje sistema. Model definiše bezbedno stanje sistema matricom pristupa – (**M**) koju čine: (redovi – **subjekti** (**S**), kolone – **objekti** (**O**) i ćelije matrice – **atributi** prava pristupa (**A**) za korišćenje **O** od strane **S**.

Dakle, ćelije matrice se mogu definisati sa:

$$M(S,O) = A,$$

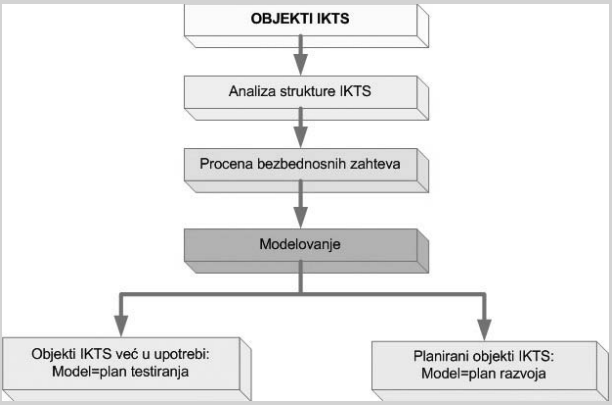
što znači da subjekat **S** ima prava pristupa i korišćenja tipa **A** na objektu **O.**

Svakom **O** u sistemu pridružuje se *referentni monitor*, poseban kontrolni program koji kontroliše pristup do tog **O** na sledeći način:

- subjekat **S** zahteva pristup do objekta **O** na način **a**,
- operativni sistem kreira trojku **(S,O,a)** i dostavlja je programu referentnog monitora za objekat **O**,
- monitor upoređuje atribute pristupa **A(S,O)** iz matrice pristupa, primenjujući zahtev **a**,
- ako je **a** jedan od atributa, pristup je dozvoljen, ako ne – odbija se.

Primer 3: strukturno modelovanje arhitekture sistema zaštite RM smanjuje kompleksnosti u četiri koraka:

1. Korak: Analiza mrežnog plana i uklanjanje svake informacije, koja nije neophodna za *sistem osnovne zaštite,* vrši se kroz procedure za pripremu i reviziju plana topologije, redukciju kompleksnosti identifikovanjem grupa sličnih objekata i skupljanje informacija o IKTS. Uloga *modelovanja sistema osnovne zaštite IKTS* u procesu razvoja sistema zaštite prikazana je na Sl. 3.2. [6].



Sl. 3.2. Izlaz modelovanja sistema osnovne zaštite IKTS

2. Korak: Ažuriranje mrežnog plana ili delova plana, sa stvarnim stanjem topologije RM i kombinovanje identičnih komponenti u jednu grupu, koja se u strukturnom modelu predstavlja jednim objektom. Komponente RM mogu biti grupisane u istu grupu ako su *sve istog tipa i imaju identične ili skoro identične osnovne konfiguracije, povezane u mreži na isti ili skorio isti način (*npr. na isti komutator*), nalaze se u istim administrativnim, infrastrukturnim i bezbednosnim uslovima, koriste iste aplikacije itd.* Ako su ovi uslovi ispunjeni onda uzorak jedne grupe može biti predstavnik bezbednosnog stanja grupe u celini. Najznačajniji momenat u grupisanju objekata IKTS je grupisanje servera i klijentskih računara. Obično u organizaciji postoji veliki broj računara, koji se može smanjiti na upravljiv broj grupa, ako se sledi navedena procedura. Kada se grupisanje svih komponenti RM izvrši, svaka grupa je jedinstvena *zona bezbednosti,* koja se u planu predstavlja sa po jednim objektom za zaštitu.

3. Korak: Definisanje kategorija bezbednosnih ciljeva za svaku zonu na bazi zajedničkih pretnji. Gubici koji mogu nastati, zbog gubitka **CIA** informacija, tipično se mogu grupisati u sledeće scenarije pretnji [6]: *povreda zakona, regulativa ili ugovora, gubljenje ili smanjenje tačnosti informacija, fizičke povrede, gubljenje ili slabljenje radnih rezultata, negativni efekti na ugled organizacije i finansijske posledice.* Često jedan slučaj može uključiti nekoliko kategorija gubitaka. Na primer, pad aplikacije može sprečiti da se izvrši bitan poslovni zadatak, izazvati finansijski gubitak i gubitak ugleda. Da bi se povukle jasne granice između kategorija bezbednosnih ciljeva *nizak, srednji, visok* (ili druge slične granulacije), treba definisati gornje i donje granice za svaki individualni scenario pretnji.

4. Korak: Grupisanje istih ili sličnih kategorija bezbednosnih zahteva u zajedničke zone bezbednosti sa istim bezbednosnim ciljem, radi smanjenja kompleksnosti. Zatim se jedinstveno opisuje svaki tip objekta u svakoj bezbednosnoj zoni i formira matrica koja sumira tokove važnih podataka između zona. Glavne prednosti definisanja *bezbednosnih zona* su smanjenje kompleksnosti IKTS za sve aspekte zaštite, pojednostavljenje dijaloga sa upravom i grupisanje sistema/objekata sa sličnim bezbednosnim zahtevima (**Prilog 3**) [74].

U klasičnom objektnom pristupu, strukturno modelovanje je zastarelo najmanje iz dva razloga: (1) podele na aktivne (*subjekte*) i pasivne (*objekte*) i (2) što se svaki program (metod) realizuje od strane konkretnog korisnika. Realizacija *objekta* je složena, jer objekat ispunjavanja volju korisnika i uvek se može smatrati da korisnik direktno ili indirektno na svoj rizik zahteva od nekog objekta određeni servis.

U *tradicionalnom pristupu zaštiti* važan zahtev je bezbednost ponovljenog korišćenja *objekata* (pasivnih nosilaca informacija, kao što su dinamičke memorije itd.), što je u konfliktu sa fundamentalnim principom dekompozicije objekata. Takav *objekat* nije moguće sanirati metodom prepisivanja (naizmeničnih 0 i 1), osim ako sam ne sadrži odgovarajući metod. Ukoliko takav metod postoji, pouzdanost čišćenja memorije zavisi od korektnosti njegove realizacije. Osnovni problem strukturnog pristupa je u tome što nije primenljiv u ranoj fazi analize i modelovanja, kada se do algoritma i funkcije dekompozicije još nije stiglo. Zato je nužno uvesti model „šireg spektra" – OOM, koji nema takve konceptualne razlike sa realnim sistemima, a može se primenjivati u svim fazama razvoja kompleksnih sistema [21].

3.3.2. Objektno orijentisano modelovanje sistema zaštite

Znanja i iskustva iz OOM, na kojem se zasniva *projektovanje* savremenih IKTS i predstavlja isproban SE metod za smanjivanje kompleksnosti sistema, slabije se koriste u oblasti zaštite informacija. Svaki racionalan metod za smanjenje kompleksnosti primenjuje *princip dekompozicije* u manji broj relativno nezavisnih objekata sa minimalnim brojem njihovih veza. OOM koristi dekompoziciju strukture IKTS na *objekte*, tj. ponašanje sistema opisuje se terminima međusobnih dejstava *objekata*, pri čemu nema pasivnih,

već su svi objekti aktivni, a po potrebi izazivaju načine ponašanja jedan drugoga. Detalji realizacije tih ponašanja su skriveni (*inkapsulirani*), a povezivanje objekata dostupno je samo interfejsu. Za razumevanje pojma *objekta* IKTS zahteva se razumevanje *klasifikacije i kategorizacije* objekata i uvođenje pojma *klase* objekata. Generički, *klasifikacija* bilo kojih objekata mora da ima sledeće atribute [81]:

- *međusobnu isključivost:* sprečava preklapanja ili klasifikaciju u jednu kategoriju;
- *potpunost:* unija svih kategorija obuhvata sve moguće klasifikacije;
- *nedvosmislenost:* svaka klasifikacija mora biti jasna i precizna;
- *ponovljivost:* svaki proces klasifikacije mora biti ponovljiv – da daje isti rezultat;
- *prihvatljivost*: svaka klasifikacija mora biti logična i intuitivna;
- *primenljivost:* klasifikacija mora biti primenljiva u različitim oblastima.

U kontekstu sistema zaštite, pod *bezbednosnom kategorizacijom* podrazumeva se klasifikacija objekata IKTS u kategorije sa istim bezbednosnim ciljevima, na koje se mogu primeniti svi navedeni atributi klasifikacije. *Bezbednosna klasifikacija informacija* se odnosi na bezbednosne nivoe informacija (npr. *interne, poverljive, strogo poverljive, državna tajna)* [25, 61].

Klasa je apstrakcija skupa stvarnih karakteristika realnog sveta, objedinjenih jednakom *opštom strukturom i ponašanjem*. *Objekat* je elemenat klase, tj. apstrakcija određene stvarnosti. Objekti su aktivni elementi, koji imaju unutrašnju strukturu i način ponašanja, koji se opisuje tzv. *metodom objekta*. Na primer, može se odrediti klasa „*korisnika*", koja označava opšti pojam korisnika sa opštim korisničkim podacima i metodama ponašanja, a zatim objekat – „*korisnik XY*" sa odgovarajućim konkretnim podacima i moguće posebnim načinom ponašanja. Značajni pojmovi OOM zaštite su *inkapsulacija, nasleđivanje, polimorfizam, grane objekta, nivo dekompozicije, komponente objekta i kontejner* [21].

- *Inkapsulacija* komponenti objekta, osnovni instrument smanjenja kompleksnosti sistema, podrazumeva skraćivanje unutrašnje strukture objekta, detalja realizacije i metoda ponašanja i smanjivanje složenosti realizacije, održavajući vidljivim samo značajne interfejse na datom nivou aproksimacije.
- *Nasleđivanje* je formiranje nove klase objekata na osnovu postojeće, sa mogućnošću dodavanja ili ponovnog određivanja podataka i načina ponašanja. Dopušta razvoj komponenti u ranoj fazi razvoja sistema, ne narušavajući integritet složenog objekta. Važan je faktor smanjenja multiplikativnih elemenata realnog sistema, gde se opšta informacija ne duplira, nego se samo ukazuje na postojeće promene, čime klasa-potomak postaje koren nove klase-naslednika.
- *Polimorfizam* je sposobnost objekta da se svrsta u više od jedne klase, što zavisi od aspekta i kriterijuma posmatranja objekta i omogućava grupisanje objekata sa sličnim karakteristikama. Važno je uočiti da nasleđivanje i polimorfizam zajedno, omogućavaju modularnu nadogradnju OOM.

- *Grane objekta* su relativno nezavisne karakteristike realnog objekta, koje smanjuju kompleksnost zaštite i bolje od polimorfizma omogućavaju raznolikost aspekata apstrakcije i posmatranja objekata. Za struktuiranje bezbednosnog cilja razvoja *integrisanog sistema zaštite informacija* i smanjenje kompleksnosti, uvode se skupovi *grana objekata*:
- grane informacionih objekata: *raspoloživost, integritet i poverljivost informacija* (CIA), koje možemo smatrati relativno nezavisnim i, ako su sve tri obezbeđene, smatra se da je obezbeđen i zaštićen IKTS i
- grane objekata sistema zaštite: *upravljačke, organizaciono-operativne* i *tehničke kontrole zaštite*.

Obe grane objekata razmatraju se sa različitim nivoima detalja. Zakoni, normativi i standardi odnose se na sve subjekte u informacionom okruženju, dok se administrativne mere odnose na sve subjekte u predmetnoj organizaciji. Proceduralne mere se odnose na pojedince ili grupe korisnika – ljudi u okviru IKTS, a hardversko-softverske – na tehničke mehanizme i protokole zaštite. Prelaskom sa jednog na drugi nivo zaštite primenjuje se karakteristika *nasleđivanja* – svaki sledeći nivo se ne menja, nego dopunjuje sa prethodnim nivoom zaštite, što omogućava *koncept slojevitosti zaštite* i *polimorfizam* (npr. subjekti u različitim ulogama – administratori zaštite, obični korisnici...).

Na ove relativno nezavisne grane deluje i princip *inkapsulacije*, što suštinski označava da je svaka grana *relativno nezavisna*. Ova dva skupa grana možemo nazvati *ortogonalnim*, pošto za fiksnu granu u jednom skupu (na primer, *raspoloživost*), treba razmatrati sve elemente iz drugih skupova (proceduralnih i tehničkih kontrola). Dva ortogonalna skupa sa brojem elemenata od tri daje osam kombinacija ortogonalnih skupova, što je još uvek prihvatljiv nivo kompleksnosti.

- *Nivo dekompozicije* je važan, ne samo za vizuelizaciju, nego i za sistemsku analizu složenih objekata, predstavljenu u hijerarhijskoj formi. Koncept dekompozicije je jednostavan: *ako se tekući nivo hijerarhije razmatra sa nivoom detalja* ***n>0****, sledeći se razmatra sa nivoom detalja* ***(n–1);*** *objekat sa nivoom detalja* ***0*** *smatra se atomizovanim (nedeljivim); nivoi detalja variraju za objekte i za grane objekta.*
- *Komponenta objekta* se može definisati kao višestruko korišćeni sastavni elemenat objekta, koji ima sve karakteristike OOM.
- *Kontejner* sadrži više komponenti i formira opšti kontekst međudejstava sa drugim komponentama i okruženjem. Jedan kontejner može imati ulogu komponente drugog kontejnera. Pojmovima komponente i kontejnera mogu se na suštinski način predstaviti istovremeno sistem zaštite i objekti IKTS koji se štite, posebno, pojam kontejnera može odrediti *granice zone zaštite* (*perimetar* ili *domen* zaštite).

3.4. REZIME

Strategija zaštite obezbeđuje okvir za razvoj sistema zaštite za dugoročne bezbednosne ciljeve. Razvoj i implementacija programa i sistema zaštite uključuju koncepte *metodologije, tehnologije, operativne prakse* i *odgovornos*ti u zaštiti.

Metodologije i okviri u oblasti zaštite se grupišu zajedno, najčešće kao *upravljačke kontrole*, pošto dodaju strukturu procesima zaštite, a uspostavljaju se na osnovu internih i eksternih (industrijskih) standarda. Oba konteksta su jednako značajna. Svaka metodologija u potpunosti je određena, definisanjem *principa, modela, metoda upotrebe i toka razvoja procesa***.**

Opšta metodologija za razvoj sistema zaštite generalno koristi: politiku zaštite, procenu rizika, standarde najbolje prakse zaštite i njihove kombinacije. Za razvoj sistema zaštite mogu se koristiti brojni klasični modeli za projektovanje IKTS i procenu rizika (SDLC, vodopada, sa brzim odzivom i dr.), ali bolje rezultate daju *strukturni* i *OOM*, čija je osnovna prednost smanjenje kompleksnosti.

Strukturni model u kojem subjekti izvršavaju dozvoljene aktivnosti nad objektima sistema, protive se algoritamskoj dekompoziciji, kojom se sistem deli na funkcionalne objekte i prikazuje *funkcionalnim modelom*. Osnovni problem strukturnog pristupa je što nije primenljiv u ranoj fazi analize, kada se do algoritma i funkcije dekompozicije još nije stiglo. Takve zahteve zadovoljava *OOM*, koji nema konceptualne razlike sa realnim sistemima i može se primenjivati u svim fazama razvoja kompleksnih sistema.

OOM karakterišu *inkapsulacija*, *nasleđivanje* i *polimorfizam*. Za struktuiranje bezbednosnog cilja razvoja integrisanog sistema i smanjenje kompleksnosti zaštite informacija, uvode se *grane informacionih objekata* (CIA), a za struktuiranje sredstva za postizanje tog cilja – *grane objekata sistema zaštite* (U,O,T kontrole).

3.5. KLJUČNI TERMINI

Metodologija: nauka o metodama; sistem organizovanja principa, modela (koncepata), metoda, tehnika i alata, toka procesa (redosleda aktivnosti) i kontrola razvoja procesa.

Model: aproksimacija realnog sistema, koja najpribližnije predstavlja tokove procesa, funkcionisanje i/ili druge relevantne atribute realnog sistema.

Objekat zaštite: fizički/logički objekti informacione imovine, koji se štite implementiranim sistemom zaštite.

Okvir: ambijent u kojem se nešto rešava (zakonski, normativni, metodološki).

Pouzdanost: funkcionalno-operativna, etinička mera korektnog funkcionisanja u propisanim granicama komponenti, uređaja, podsistema i sistema u operativnom radu.

Procedura: definisan i uspostavljen način rada i odvijanja procesa korak po korak.

3.6. PITANJA ZA PONAVLJANJE

1. Metodologije i okviri su:
   a. upravljačke kontrole koje dodaju strukturu procesima zaštite
   b. grupišu se zajedno, najčešće kao upravljačke kontrole
   c. grupišu se zajedno, najčešće kao operativne kontrole
   d. razvijaju se na bazi internih i/ili opšte prihvaćenih industrijskih standarda
   e. uspostavljaju se u kontekstu organizacije za svaki projekat zaštite
2. Strategija zaštite:
   a. obezbeđuje okvir za kratkoročne bezbednosne ciljeve sistema zaštite
   b. sadrži konsolidovanu viziju tekućeg i željenog bezbednosnog stanja sistema
   c. uključuje indikatore za praćenje progresa i presek stanja sistema zaštite
   d. uključuje akcioni plan za izvršavanje taktičkih ciljeva zaštite
3. Za razvoj programa i sistema zaštite, generalno se koriste metodologije na bazi:
   a. politike zaštite
   b. SDLC (razvoja životnog ciklusa)
   c. upravljanja rizikom
   d. najbolje prakse zaštite
   e. ISO/IEC 21827 i ISO/IEC 27001
4. Standardne metodologije i okviri zaštite odgovaraju:
   a. u potpunosti za projektovanje savremenih IKTS sistema
   b. u potpunosti za projektovanje sistema za e-poslovanja i *Cloud Computing*
   c. samo ako su kombinovani i prilagođeni kontekstu i okruženju organizacije
   d. samo ako su usaglašeni sa normativima zaštite
5. Osnovne komponente strukturnog modela bezbednog IKTS su:
   a. skup pasivnih i aktivnih *objekata,* kojima se pristupa na kontrolisan način
   b. skup aktivnih *subjekata*, koji koriste i pristupaju *objektima*
   c. skup *pravila* na osnovu kojih subjekti koriste i pristupaju objektima
   d. skup aktivnih *objekata*, koji koriste i pristupaju objektima IKTS
   e. skup objekata čije se ponašanje opisuje njihovim međusobnim dejstvima
6. Osnovni koraci u procesu strukturnog modelovanja IKTS i sistema zaštite su:
   a. analiza i ažuriranje topologije mrežnog plana i grupisanje komponenti istog tipa u istu grupu
   b. analiza plana zaštite, ažuriranje topologije mrežnog plana i određivanje zona bezbednosti,
   c. određivanje troškova zaštite i grupisanje komponenti istog tipa u istu grupu
   d. grupisanje istih/sličnih kategorija bezbednosnih zahteva u zajedničke zone bezbednosti
   e. definisanje kategorija bezbednosnih zahteva/ciljeva za svaku zonu
7. *Grane informacionih objekata* u OOM sistema zaštite obuhvataju:
   a. raspoloživost, poverljivost, integritet i autentifikaciju
   b. upravljačke kontrole, raspoloživost, poverljivost, integritet i autentifikacija
   c. upravljačke, tehničke i organizaciono – operativne kontrole
   d. raspoloživost, poverljivost, integritet
8. Grane *objekata za zaštitu* u OOM sistema zaštite obuhvataju:
   a. raspoloživost, poverljivost, integritet i autentifikacija
   b. upravljačke kontrole, raspoloživost, poverljivost, integritet i autentifikacija
   c. upravljačke, tehničke i organizaciono – operativne kontrole
   d. raspoloživost, poverljivost i integritet
9. Strukturna svojstva OOM su::
   a. inkapsulacija, nasleđivanje, polimorfizam, grane objekta, nivo dekompozicije, komponente objekta i kontejner zaštite
   b. inkapsulacija, polimorfizam, grane objekta, nivo dekompozicije i kontejner zaštite
   c. inkapsulacija, nasleđivanje, polimorfizam, grane objekta, komponente
   d. objekta i definisanje programa zaštite
10. Procesni razvoj sistema zaštite zahteva:
    a. neformalni opis procesa zaštite
    b. definisanje procesa zaštite
    c. kontrolu i poboljšavanje procesa zaštite
    d. formalni opis procesa zaštite

4. KONCEPTI SISTEMA I KONTROLE ZAŠTITE

Po završetku ovog poglavlja razumećete:

- Prednosti i nedostatke koncepata reaktivne i proaktivne zaštite
- Značenje termina i namenu kontrola zaštite
- Strukturu upravljačkih, operativnih i tehničkih kontrola
- Metod izbora kontrola zaštite za sistem osnovne zaštite
- Metod bezbednosne kategorizacije i klasifikacije

4.1. UVOD

Misija *sistema zaštite* je da održava bezbednosno stanje informacija i IKTS na prihvatljivom nivou rizika. U praksi se zahteva *izbalansirana i komplementarna zaštita,* u kojoj se manje efikasne i efektivne *kontrole* zamenjuju sa efikasnijim i efektivnijim, a *tehničke* dopunjuju sa *proceduralnim* kontrolama.

Primena samo tehničkih kontrola predstavlja parcijalno rešenje *reaktivne* zaštite ili "popravku" sistema od poznatih ranjivosti i pretnji. Prema podacima NIST–a (2008), oko 99% svih registrovanih upada u IKTS, rezultat su korišćenja poznatih ranjivosti OS ili grešaka konfiguracije, za koje su bile na raspolaganju *kontrole zaštite*, ali nisu implementirane. Ovo, kao i slučajni karakter uticaja dinamički promenljivih i kombinovanih pretnji na informacionu imovinu i poslovanje, zahtevaju *proaktivnu* zaštitu od poznatih i nepoznatih ranjivosti i pretnji.

Cilj definisanja koncepta *kontrola zaštite* je da se, na osnovu rezultata procene rizika, obezbede skupovi skalabilnih *upravljačkih (U), operativnih (O) i tehničkih (T)* kontrola za *osnovni*, *poboljšani* i *visoki nivo* zaštite.

4.2. KONCEPT SISTEMA REAKTIVNE ZAŠTITE

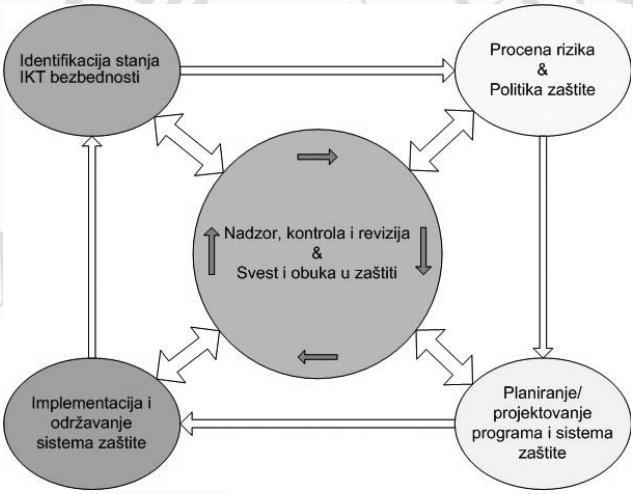
4.2.1. Sistem reaktivne zaštite

Koncept *reaktivne zaštite* je zaštita od *poznatih ranjivosti i pretnji.* Sistem r*eaktivne zaštite* u većini slučajeva kasni, a nove sofisticirane tehnike napada čine nekorisnim prethodno ažurirane definicije virusa u AVP. Reaktivna zaštita je tipična za većinu IDS sistema, ali ne i za savremene IDPS sisteme [87].

U praksi se najčešće događa incident koji nije planiran i za kojeg se misli da se nikada neće dogoditi. Sistem zaštite se vrlo često razvija neplanirano, kao reakcija na poslednji napad ili vanredni događaj (VD), ili neusklađeno sa procenom rizika i potrebama, čime se stvara redundantan i skup reaktivni sistem zaštite. Takođe, primena samo **T** *kontrola* predstavlja parcijalno rešenje *reaktivne* zaštite, gde *popravljeni* sistem ostaje sa ranjivostima. Ipak, u sistemu reaktivne zaštite brojne aktivnosti imaju *proaktivni karakter,* kao što su *odluka menadžmenta za uvođenje sistema zaštite, primena nekog metoda za procenu rizika, izbor optimalnih kontrola, razvoj svesti o potrebi zaštite, podrška menadžmenta i dr.* [61].

4.2.1.1. Funkcionalni model reaktivne zaštite

Funkcionalni model (Sl 4.1) sistema reaktivne zaštite sadrži sledeće glavne faze: *identifikaciju stanja zaštite, procenu rizika, planiranje i implementaciju poboljšanih kontrola zaštite, operativno održavanje, nadzor, reviziju, obuku i obrazovanje* [61].



Sl. 4.1. Funkcionalni model sistema reaktivne zaštite

Opšti funkcionalni modeli *upravljanja sistemom reaktivne zaštite* može se definisati na više načina i sa različitih aspekata. Sa *metodološkog aspekta*, upravljanje sistemom reaktivne zaštite najbolje se može predstaviti procesom upravljanja rizikom u IKTS, koji obuhvata faze *planiranja, izbora T kontrola, modela zaštite, razvoja/akvizicije i selekcije kontrola i izrade uputstva za upravljanje rizikom/sistemom zaštite* [63].

Upravljanje sistemom reaktivne zaštite u RM OSI (*Open System Interchange*) modela, mora odražavati sva saopštenja politike zaštite. Entiteti koji su obuhvaćeni jedinstvenom

politikom zaštite, u sistemu kojeg administrira jedan autoritet, organizuju se u jedinstveni *domen zaštite*. Primeri *procesa* upravljanja sistemom zaštite su *distribucija kriptografskih ključeva, izveštavanje o incidentu, aktiviranje/dezaktiviranje servisa zaštite, implementacija politike zaštite* i sl.

Baza *podataka zaštite* (BPZ) je skladište svih relevantnih informacija za upravljanje sistemom višeslojne zaštite. Svaki krajnji sistem treba da sadrži lokalne informacije za primenu politike zaštite. Najčešće je BPZ distribuirana, u meri neophodnoj da se primeni konzistentna politika zaštite u krajnjim sistemima. U praksi zaštite, delovi BPZ mogu, ali ne moraju, biti integrisani u bazu podataka IKTS. BPZ se može realizovati kao relaciona baza podataka i datoteka ili sa pravilima unutar softvera ili hardvera realnog OSI sistema.

4.2.1.2. Ocena kvaliteta sistema reaktivne zaštite

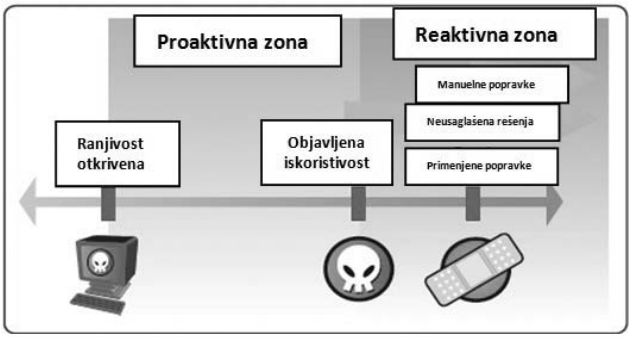
U sistemu reaktivne zaštite, organizacije u Internet okruženju tipično primenjuju tri moguća, u suštini reaktivna, rešenja i to da: (1) *ne preduzimaju ništa, (2) primenjuju manuelne ili polu–automatizovane metode bezbednosnih popravki (patches) ili (3) izvrše „ad hok" samozaštitu sa izolovanim tehničkim rešenjima na distribuiranim tačkama IKTS.*

Metod *„ne preduzimati ništa"* najčešće se zasniva na uverenju *„da se to neće baš nama dogoditi* i sl". Nažalost, pravi dokaz o postojanju pretnje obično dolazi, posle uspešno izvršenog napada sa nekim gubitkom. Slično je kada IKTS ima samo logičku mrežnu barijeru (*firewall*) ili neku drugu statičku formu infrastrukture zaštite, koja ne pruža dovoljnu zaštitu za *online* režim rada [21].

Manuelna i improvizovana metoda bezbednosnih popravki ranjivosti predstavlja stari metod reaktivne zaštite. Teoretski je moguće pratiti sve potencijalne izvore pretnji, preuzeti sve relevantne bezbednosne popravke *ranjivosti* i zatim testirati i instalirati svaku od njih, na svakom potencijalno ugroženom RS. Međutim, potrebno je značajno vreme za identifikovanje, manuelno fiksiranje i testiranje potencijalno ranjivih RS u mreži, što je kritično u slučaju neposrednog rizika od napada sa Interneta. U odnosu na prvu opciju, ni ovo rešenje ne obezbeđuje valjanu strategiju zaštite. Vremenski prozor reaktivne zone zaštite, sa različitim rešenjima i manuelnim otklanjanjem ranjivosti, nalazi se između vremena objavljivanja iskorišćenja određene ranjivosti i manuelne popravke te ranjivosti (Sl. 4.2) [53].

Neusaglašena rešenja zaštite na izolovanim, distribuiranim tačkama IKTS su relativno spora i skupa, a trenutno preovlađuju u svetu. Obuhvataju slojevitu zaštitu po dubini, na više nivoa i sa više različitih komponenti zaštite. Upravljanje ovakvim sistemom vremenski je zahtevno, skupo i kompleksno. Rešenje je efektivno za jednokratnu upotrebu, ali ne obezbeđuje koherentnu, integralnu i uniformnu zaštitu IKTS. Bez centralizovanog upravljanja ovaj sistem ne obezbeđuje analizu i vremensku korelaciju velikog broja bezbednosno relevantnih podataka i njihovu razmenu u realnom vremenu, pa

su organizacije primorane da samostalno reaguju na bezbednosne incidente i preduzimaju skupe mere za oporavak sistema.



Sl. 4.2. Vremenski prozori proaktivnih i reaktivnih sistema zaštite [53]

Sve mere zaštite u reaktivnoj zoni usmerene su na reaktivno saniranje i oporavak sistema. Manuelne popravke ostaju u reaktivnoj zoni, a često se ne apliciraju duže vreme od objavljivanja iskoristivosti. U ovoj zoni se nalaze i različita rešenja postojećih sistema reaktivne zaštite, od kojih se većina fokusira na otkrivanje ranjivosti sistema. Pre nego što saniraju ranjivost, moraju utrošiti vreme na njeno otkrivanje, analizu i objavljivanje popravke. Administratori zaštite nemaju realne mogućnosti da izdvoje kritične ranjivosti od minornih, a običan IDS preduzima aktivnosti, tek kad je proces napada u toku. Osim toga, za analizu incidenta podaci se manuelno skupljaju sa različitih tačaka i u raznim formatima iz log datoteka distribuiranih RS, što znatno usporava i otežava analizu. Manuelne i polu–automatske popravke ranjivosti sistema, danas su standardni metodi koji obezbeđuju *nedovoljno jaku*, ali *kontrolisanu zaštitu na prihvatljivom nivou rizika*. Reaktivni sistemi zaštite troše velike resurse za planiranje, bekapovanje i oporavak sistema od, često, samo jednog napada. Rešenje je da se implementira rentabilna *proaktivn*a detekcija napada i IKTS štiti od *poznatih i nepoznatih* pretnji.

4.3. KONCEPT SISTEMA PROAKTVNE ZAŠTITE

Prvi korak u razvoju sistema *proaktivne zaštite* je korišćenje baza znanja (npr, ISC CBK *(International Security Consorcium – Common Body of Knowladge*) i drugih servisa najbolje prakse zaštite, koji omogućavaju korisnicima sopstvenu implementaciju i upravljanje zaštitom. U ovim bazama znanja uskladištene su, definisane i opisane U, O i T *kontrole najbolje prakse zaštite* za *niske, srednje i visoke* nivoe rizika.

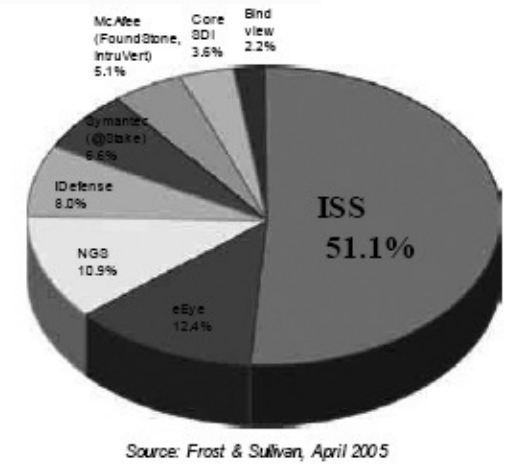
Koncept *sistema proaktivne zaštite* obezbeđuje zaštitu od iskorišćenja *poznatih* i *nepoznatih* ranjivosti, zaustavljanjem malicioznih napada na samom izvoru nastanka. Koristi najsavremenije tehnologije zaštite i *proaktivne* mere *ranog otkrivanja, predviđanja i sprečavanja* malicioznih napada, npr. *IBM Proventia® Desktop Endpoint Security* je dizajniran da zaustavi napad pre nego se dogodi [41].

Sistem *proaktivne zaštite* obezbeđuje veću rentabilnost vremena i troškova od postojećih reaktivnih sistema. Idealan zahtev je da sistem zaštite reaguje maksimalno brzo i precizno na kombinovane, dinamički promenljive pretnje (DPP).

4.3.1. Funkcionalni model proaktivne zaštite

Metod proaktivne zaštite obuhvata mehanizme zaštite na više nivoa, sa različitim brzinama reakcije i tačnosti, sa većom ukupnom efektivnošću, redukovanim operativnim rizikom i znatno nižim troškovima razvoja, rada i održavanja. Koncept sistema DPP zaštite nudi novi proaktivni pristup, u kojem se zaštita realizuje kombinacijom *baza znanja*, *vrhunske tehnologije* za *proaktivnu* zaštitu, *procesnog pristupa i pojednostavljenog rešenja sistema zaštite* [53,41].

Baze znanja vodećih obaveštajnih mreža CIRT i CERT (npr. *X–TaskForce,* **IBM ISS** – *Internet Security System*), prikupljaju podatke o pretnjama i ranjivostima sistema i obezbeđuju ažuran bilten podataka (X–*Press Updates*) u kojem se objavljuje oko 45% ranjivosti aktuelnih sistemskih programa u svetu ili 3 puta više od ostalih. *X–Force* detaljno opisuje brojne ranjivosti sistema. Na Sl. 4.3. prikazan je procenat ukupno otkrivenih visoko rizičnih ranjivosti u svetu u periodu 1998–2005. godie [53].



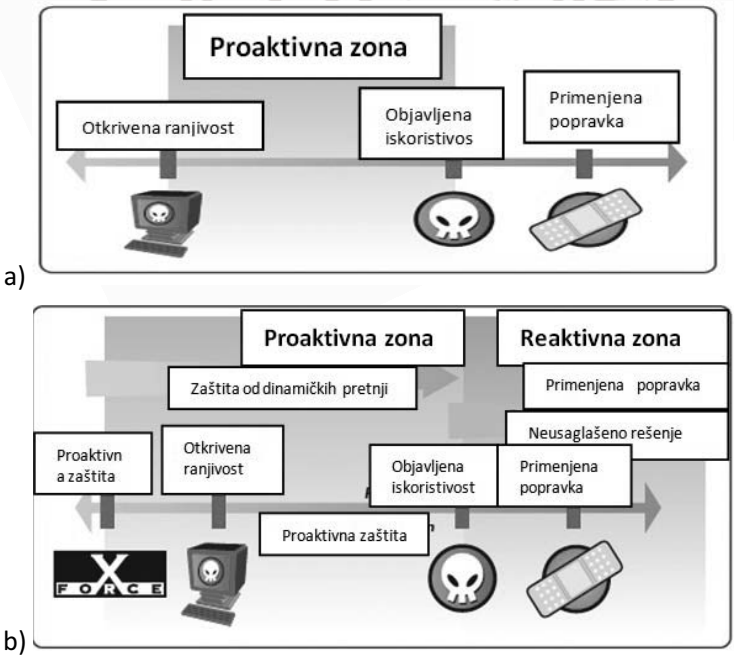
Sl. 4.3. Procenat otkrivanja ranjivosti IKTS u periodu 1998–2005. [53]

- **Vrhunska tehnologija višeslojne proaktivne zaštite** obezbeđuje automatizaciju ciklusa zaštite sa elementima ekspertnih sistema, a tipično obuhvata [41, 53]:
- **uređaj za zaštitu** (*Protection Engine),* koji sadrži *IDPS* i *Modul za reagovanje na incidente* i obezbeđuje nelinearnu zaštitu i upravlja sa IDPS,
- **uređaj za zaštitu lokacije** (*Site Protector*), koji obezbeđuje komande i centralizovano upravljanje događajima i mehanizmima zaštite u RM i RS,
- **integrator sistema** (*Fusion System),* koji vrši obradu signala, obezbeđuje prepoznavanje obrazaca i analizira uticaje DPP napada,
- **modul za ažuriranje** *(X–Press Updater*), koji automatski ažurira bazu podataka sa podacima CERT/CIRT timova.

DPP Protection Engine obezbeđuje realizaciju mehanizama DPP zaštite, a ugrađuje se u sva rešenja IBM ISS kao što su: *skeneri sistema zaštite, IDPS* (tipa *RealSecure 10/100, RealSecure Gigabit Network, RealSecure_Nokia, RealSecure_Crossbeam, ProventiaA...),* softversko–hardverski sistemi za sprečavanje napada (*ProventiaG),* višefunkcionalni uređaji za zaštitu (*ProventiaM*), IDPS servera (*Real Secure server*) i IDPS radne stanice (*Real Secure Desktop*) [41, 53].

Procesni pristup zaštiti i pojednostavljeni proces zaštite, bitne su komponente koncepta proaktivne DPP zaštite. Borba protiv nepoznatih pretnji zahteva brzo reagovanje na tek otkrivenu iskoristivu ranjivost, pre nego je neka pretnja iskoristi. Rešenja DPP zaštite koriste jedinstveni mehanizam *virtuelne zakrpe (Virtual Patch)* za automatsko fiksiranje poznatih i potencijalnih ranjivosti sistema. Na primer *IBM/ISS Proventia***,** radi tako što obezbeđuje privremeni zaklon ili "*virtuelne bezbednosne popravke"* za *zaštitu u nultom danu; sprečavaju iskorišćenje ranjivosti od poznatih i nepoznatih pretnji; ne oslanjaju se na definicije AVP, eliminišu potrebu hitnih popravki, otklanjaju rizik štete od popravki i omogućavaju primenu popravki u toku održavanja sistema i uobičajenih napada*.

Ovaj mehanizam omogućava organizaciji da trenutno, u realnom vremenu, zaštiti sistem od poznatih i nepoznatih napada, često znatno ranije od zvaničnog generisanja i objavljivanja popravki za nove ranjivosti sistema. Na slici 4.4a. na vremenskoj osi prikazana je zona *proaktivne zaštite* [53].



Sl. 4.4. Zona - (a) i prošireni prozor proaktivne zaštite – (b) [53]

Proces proaktivne zaštite počinje sa trenutkom otkrivanja/objavljivanja ranjivosti sistema. Zatim sledi generisanje napada, koji može iskoristiti otkrivenu ranjivost sistema, ali obavezno ne mora. Konačno, generiše se i aplicira nova bezbednosna popravka za otklanjanje ove iskoristive ranjivosti. Iako je vreme od otkrivanja do iskorišćenja ranjivosti promenljivo, popravka se često aplicira tek kada je šteta već naneta, zbog *potrebnog vremena za manuelnu popravku distribuiranih ranjivosti, raspoloživosti popravki za nove ranjivosti, tek kada su ranjivosti iskorišćene i sve kraćeg vremena između otkrivanja ranjivosti i njenog iskorišćenja.*

U vremenu od otkrivanja do iskorišćenja ranjivosti, nalazi se prozor proaktivne zaštite. U tački otkrivanja ranjivosti sistema aktivira se *Virtual Patch* proces, aktivira sistem za proaktivnu zaštitu i obezbeđuje zaštitu i bez poznavanja informacije o iskoristivosti te ranjivosti, koja se može generisati znatno kasnije. Dakle, zonu proaktivne zaštite od DPP (Sl. 4.4a) obezbeđuje *Virtual Patch* proces, koji štiti sistem od *nepoznatih* pretnji. U stvari, proaktivna zona zaštite se proteže i na zonu pre otkrivanja ranjivosti sistema (Sl. 4.4b), što omogućavaju stalni procesi istraživanja i dubokog razumevanje prirode ranjivosti IKTS, sistem ranog upozorenja o otkrivenim ranjivostima (ISS – obično 30 dana pre javnog otkrivanja, a 24 sata ranije od drugih entiteta) i sistem automatskog ažuriranja bezbednosno relevantnih informacija, dobijenih od istraživačkog CERT tima.

Dakle, *Virtual Patch* proces obezbeđuje rezervno vreme do pojave dovoljno ažurne bezbednosne popravke, koja ne zahteva individualno krpljenje i manuelno restartovanje sistema; redefiniše bezbednost sistema tako da se operacije zaštite izvršavaju kao deo normalnog procesa upravljanja promenama IKTS, što omogućava mnogo efektivnije i efikasnije planiranje resursa i brže reagovanje na poznate i nepoznate pretnje.

Primer: IBM realni sistem proaktivne zaštite sadrži: *upravljanje ranjivostima, IDPS, upravljani servisi zaštite i preventivni antivirusni sistem (VPS),* koji se instalira na mrežnoj kapiji i PC računarima, prati realne napade, otkriva nepoznate napade (0–dana), zaustavlja trku sa napadačima i ne zahteva ažuriranje definicija AVP. *VPS na mrežnoj kapiji,* koji sprečava nove viruse da uopšte prodru u mrežu. Ova višeslojna zaštita obuhvata *kombinovane tehnologije za sprečavanje upada virusa (VPS), AVP i anti–špijunske definicije, za sprečavanje preplavljivanja bafera, IDPS usmerene na ranjivosti, personalne barijere i kontrolu aplikacija* [41].

Proaktivni sistem zaštite, u poređenju sa reaktivnim, postiže rentabilnije vreme analize i upravljanja rizikom, veću tačnost i brzinu otkrivanja i bolje sprečavanje napada. Kako pretnje i ranjivosti rastu, sistem zaštite mora biti brži, precizniji i pouzdaniji. Napadačima je za efektivan napad dovoljna margina greške od svega 1%. Centralna platforma za DPP zaštitu, obezbeđuje znatno bolju zaštitu cele RM i smanjuje kompleksnost, eliminiše lažne alarme, znatno smanjuje ukupne troškove zaštite i približava se *optimalnom sistemu zaštite*.

Proaktivni sistem zaštite zadovoljava zahteve savremenih trendova zaštite virtuelizovanog okruženja u distribuiranom Internet računarstvu (CC), mreža u razvoju, mobilnih uređaja, senzorskih sistema za fizičku zaštitu, alternativnih puteva isporuke mehanizama zaštite, upravljanja rizikom i identitetom [41].

4.4. KONCEPT KONTROLA ZAŠTITE

4.4.1. Osnovne karakteristike kontrola zaštite

Kontrola zaštite je interfejs između korisnika i mehanizma zaštite, krajnja klasifikacija mehanizma zaštite, a implicira da se svaki mehanizam zaštite mora kontrolisati. Tipično, to je neka funkcija dizajna sistema zaštite i odnosi se na *tehničke* i *proceduralne mehanizme*. Kvalitet kontrole zaštite određuju njene funkcionalne karakteristike: *robusnost* (otpornost na napade), *adaptivnost* (*fleksibilnost* – mogućnost zamenljivosti i *skalabilnost* – mogućnost proširivanja), *organizacija* i *struktura* u procesu zaštite. Kvalitet kontrole zaštite osnov je za evaluaciju kvaliteta procesa zaštite u procesu sertifikacije i akreditacije i kvaliteta garantovane bezbednosti IKTS [33, 61, 82, 83].

Robusnost kontrole definiše stepen jačine bezbednosne funkcije – nivo garantovane bezbednosti, zavisno od efektivnosti implementacije, a omogućava definisanje kontrola sa različitim intenzitetom zaštite. Određena je sa dva ključna faktora:

- *intenzitetom bezbednosne funkcije* ili relativnom merom potrebnog rada ili troškova za proboj korektno implementirane kontrole i
- *nivoom* osnove za sticanje poverenja u efektivnost kontrole, definisane sa 3 nivoa robusnosti – *osnovni* (**o**), *srednji* ili *poboljšani* (***p***)) i *visoki* (**v**).

Adaptivnost (*skalabilnost* i *fleksibilnost*) omogućava nadgradnju, poboljšanje i izbor skupa kontrola, adekvatnih za politiku zaštite i potrebe organizacije. *Skalabilnost* implicira modularnost nadgradnje kontrola, a *fleksibilnost* elastičnu primenu poznatih formi zaštite (npr. bekapovanje sedmično, mesečno, dnevno).

Struktura kontrole zaštite ima standardnu formu iz više razloga. Postoje brojni tipovi različitih kontrola zaštite, koje se mogu iskoristiti u konkretnom sistemu. Kontrole se dinamički razvijaju i menjaju u zavisnosti od promena u sistemu upravljanja, operativnom okruženju, pretnjama i tehnologijama zaštite. Struktura dokumentovane kontrole zaštite treba da sadrži sekcije: (1) *cilja* za **o, p** i **v**, zaštitu, (2) *opisa* specifičnih zahteva i detalja za **o, p** i **v** zaštitu i (3) *mapiranja* sa zahtevima za zaštitu, da se izbegne dupliranje kontrola.

Organizacija kontrola zaštite u *klase* i *familije* obezbeđuje njihovu lakšu primenu. U skladu sa OOM postoje *klase upravljačkih (***U***), operativnih (***O***) i tehničkih* (***T***) kontrola zaštite, koje sadrže *familije*, a ove – *kontrole* [83].

Klasa **U** *kontrola zaštite* odnosi se na upravljanje sistemom zaštite i rizikom i sadrži ***pet*** *familija*. Klasa **O** *kontrola* sadrži **devet** *familija,* podržava **U** i **T** kontrole, a primarno ih izvršavaju ljudi. Klasa **T** *kontrola* sadrži **četiri** *familije,* a uključuje hardversko-softverske mehanizme i protokole zaštite, koje izvršava sistem. Kontrole familije *Upravljanja programom* – PM (*Program management*) mogu se smatrati opštim kontrolama zaštite na nivou organizacije (uvedene su u rev. 3). Tipično pokrivaju više IKTS i obično se specificiraju u *planu*

zaštite, umesto u katalogu kontrola. U Tabeli 4.1. prikazane su klase, pripadajuće familije i jedinstveni identifikatori familija za srpsku i (*englesku*) konvenciju kodiranja [33, 83].

Tabela 4.1. Klase, familije i identifikatori kontrola zaštite

Identifikator	Klasa	Familija kontrola
UP (*PM*)	Upravljačka	Upravljanje programom
BA (*CA*)		Sertifikacija i akreditacija sistema zaštite
PS (*PL*)		Planiranje sistema zaštite
PR (*RA*)		Procena rizika
AS (*SA*)		Akvizicija sistema i servisa zaštite
SO (*AT*)	Organizaciono –operativna	Svest o potrebi i obuka u zaštiti
UK (*CM*)		Upravljanje konfiguracijom
PP (*CP*)		Planiranje kontinuiteta poslovanja
UI (*IR*)		Upravljanje incidentom
IS (*SI*)		Integritet sistema i informacija
OS (*MA*)		Održavanje sistema zaštite
ZM (*MP*)		Zaštita medija
FZ (*PE*)		Fizička i zaštita okruženja
PZ (*PS*)		Personalna zaštita
RO (*AU*)	Tehnička	Revizija i odgovornosti
KP (*AC*)		Kontrola pristupa
IA (*IA*)		Identifikacija i autentifikacija
ZS (*SC*)		Zaštita sistema i komunikacija

Jedinstveno kodiranje svake kontrole, primenom standardizovane konvencije, obezbeđuje *jednoznačnu identifikaciju*:

- *klase*: numeričke oznake (1, 2, 3...),
- *familije*: sa dva velika slova koja jednoznačno definišu ime familije,
- *nivoa robusnosti*: **o–**osnovna, **p–**poboljšana i **v** –visoka robusnost i
- *broj kontrole*: ispred ovog identifikatora, određuje redosled kontrole u okviru familije prema prioritetu bezbednosnog značaja.

Primer: **PZ–4.o** jedinstveno označava četvrtu kontrolu zaštite sa *osnovnim* nivoom robusnosti u familiji *Personalna zaštita*.

Dimenzije kontrola zaštite**–***životni ciklus, forma, namena, kategorija, karakteristike i parametri implementacije,* određuju njihov kvalitet (Tabela 4.2).

Tabela 4.2. Dimenzije kontrola zaštite

Dimenzija kontrole zaštite	Opis atributa
Životni ciklus	*dizajn, implementacija, održavanje, odlaganje*
Forma	*politika, procesi, tehnologija*
Namena	*prevencija, odvraćanje, detekcija, redukcija, oporavak, korekcija, monitoring, razvoj svesti*
Kategorija događaja	*kontrola gubitaka, kontrola pretnji, kontrola ranjivosti*
Karakteristike	*robusnost, fleksibilnost*
Parametri implementacije	*cena, benefiti, prioriteti*

4.4.2. Skup kontrola za sistem osnovne zaštite

Izbor adekvatnih kontrola za ispunjavanje specifičnih zahteva za zaštitu, demonstrira stvarnu odlučnost organizacije za zaštitu **CIA** informacija [48]. *Skup kontrola za sistem osnovne zaštite* je minimalan. Preporučuje ga najbolja praksa zaštite za tipičan IKTS, a obezbeđuje održavanje ukupnog preostalog rizika na prihvatljivom nivou. Rentabilne kontrole zaštite određuju se i biraju na bazi *bezbednosne kategorizacije* i *klasifikacije* informacione imovine i *procene rizika*.

Za efektivnu zaštitu treba koristiti kontrole zaštite definisane u bazama znanja i prilagoditi ih specifičnostima organizacije u formi *kataloga kontrola* [33, 83], u kojem se identifikuju tri osnovna skupa **U, O** *i* **T** kontrola, koje odgovaraju *niskom (N), srednjem (S) i visokom (V)* nivou zaštite, definisanom u procesu kategorizacije i klasifikacije. Lista kontrola za osnovnu zaštitu obezbeđuje minimum zaštite za odgovarajuću bezbednosnu kategoriju. Kontrole zaštite, u svakom od tri osnovna skupa, sadrže kombinaciju *akumuliranih* kontrola sa tri nivoa robusnosti. Na primer, za *N nivo* osnovne zaštite katalog sadrži kontrole zaštite sa osnovnim nivoom robusnosti **o**; za *S nivo* osnovne zaštite – kombinaciju kontrola zaštite sa **o** i **p** nivoima robusnosti; za *V nivo* osnovne zaštite – kombinaciju kontrola zaštite sa **o, p** i **v** nivoima robusnosti. Pri tome ne postoji direktna korelacija između tri nivoa robusnosti kontrola zaštite i tri nivoa osnovnih skupova kontrola zaštite. Odgovarajuće kontrole zaštite biraju se za odgovarajuće nivoe osnovne zaštite. Na primer, neka kontrola zaštite sa **o** nivoom robusnosti, može se prvo pojaviti na *V* nivou osnovne zaštite ili se nikada ne pojavljuje, već je samo na raspolaganju kao opcija organizaciji za dopunu skupa kontrola zaštite. Neke *kompenzujuće* ili *univerzalne* kontrole zaštite, mogu se primenjivati u sva tri osnovna skupa kontrola zaštite i za sve nivoe robusnosti. Skup kontrola za osnovnu zaštitu namenjen je za ublažavanje glavnih faktora rizika, a za *N* uticaj faktora rizika sadrži ukupno **198** (**U= 42, O= 78 i T=78**) kontrola sa *N nivoom robusnosti* [83].

Mapiranje odgovarajućih kontrola sa specifičnim zahtevima za zaštitu vrši se pomoću *matrice za praćenja bezbednosnih zahteva* – **RTM** (*Requirements Traceability Matrix*), koja se konstruiše identifikovanjem usaglašenih, specifičnih *bezbednosnih zahteva* i odgovarajućih kontrola zaštite iz izabranih skupova kontrola za osnovnu zaštitu, koje te zahteve ispunjavaju. Mapiranje može biti:

- **1:1,** jedan zahtev rešava se sa jednom kontrolom zaštite,
- **1:N,** jedan zahtev rešava se sa više kontrola zaštite,
- **N:1,** više zahteva rešava se sa jednom kontrolom zaštite i
- **N:M,** više zahteva rešava se sa više kontrola zaštite.

U Tabeli 4.3. ilustrovan je primer dela RTM matrice za hipotetičke zahteve za zaštitom i standardizovan skup kontrola iz kataloga kontrola zaštite.

Tabela 4.3. Primer matrice praćenja zahteva za zaštitom

Zahtevi zaštite	Mapiranje	Kontrole zaštite
Zahtev br. 1	1:1	PS–1o
Zahtev br. 2	1:N	PE–2o, PE–3o, PE– 6s, PE–7o
Zahtev br. 3, Zahtev br. 4	N:1	CM–2s
Zahtev br. 5, Zahtev br. 6	N:M	IA–1s, IA–2s, IA–4o

Kontrole zaštite nisu statičke kategorije i mogu se revidirati na osnovu *promena prakse, zahteva i tehnologija zaštite*. Modifikacija kontrola zaštite, mora proći rigoroznu raspravu, reviziju i konsenzus svih zainteresovanih strana u organizaciji.

4.4.3. Proces selekcije i implementacije kontrola zaštite

Izbor *optimalnih U, O i T kontrola zaštite* za ublažavanje faktora rizika na prihvatljiv nivo, važan je zadatak za svaku organizaciju. Pre izbora treba izvršiti *bezbednosnu kategorizaciju* i *klasifikaciju* informacione imovine i procenu rizika, čime se verifikuje njihova vrednost. Prva aktivnost u procesu izbora kontrola je opis faktora rizika sa liste prioritetnih rizika, koje treba ublažiti na prihvatljiv nivo. Da bi se razumeli vrsta i intenzitet pokrivanja pretnji/rizika primenjenim kontrolama zaštite, potrebno je odrediti koji se faktori rizika i sa kojim kontrolama zaštite ublažavaju, ne ublažavaju, zaobilaze ili su postali prihvatljivi preostali rizik. Za to su korisne dostupne taksonomije potencijalnih pretnji i ranjivosti IKTS. Jedna od praktičnih taksonomija je podela pretnji na *greške, prirodne događaje i namerne napade,* koji se karakterišu prema *tipu, sposobnostima, resursima i namerama napadača* [22, 63].

U izboru kontrola za *sistem osnovne zaštite*, procenjuje se pokrivanje pretnji/rizika sa kontrolama zaštite na bazi *mapiranja*: *1:1,1:N i 0:N (nemogućnost pokrivanja faktora rizika jednom ili više kontrola*). Da bi se generisale adekvatne kontrole zaštite za osnovnu zaštitu treba izvršiti analizu i procenu rizika u ranoj fazi razvoja IKTS. Ako se pokaže da su pokrivanja pretnji neadekvatna, mogu se poboljšati kontrole za osnovnu zaštitu, povećanjem njihove robusnosti ili dodavanjem novih. Proces izbora kontrola zaštite treba voditi na osnovu rezultata procene rizika. Primer metoda za procenu pokrivanja različitih pretnji osnovnim kontrolama zaštite prikazan je u **Prilogu 4** [25].

Bezbednosna klasifikacija i kategorizacija informacione imovine, informacije o sistemu (*obim, granice, dekompoziciju, kritičnost i izloženost sistema napadima itd.)* uzima iz *plana zaštite*, a na osnovu bezbednosnih zahteva [3,10, 65].

U sistemu zaštite pojam *klasifikacije* se odnosi na klasifikaciju bezbednosnih nivoa informacija (npr. *interne, poverljive, strogo poverljive, državna tajna itd.*), a informacije se svrstavaju u kategorije u odnosu na *tip informacije* (privatna, vojna, zdravstvena, finansijska, naučno–istraživačka, poslovna, diplomatska, obaveštajna itd.), koju definišu zakoni, uredbe, regulative, organizacije ili politika zaštite [21].

Pod *kategorizacijom* se podrazumeva klasifikacija svih objekata informacione imovine u bezbednosne kategorije, na koje se mogu primeniti svi generički kriterijumi klasifikacije. Standardni proces *kategorizacije* uspostavlja bezbednosne kategorije za određivanje vrednosti informacione imovine (A), koje se zasnivaju na kriterijumu *uticaja* faktora rizika na *misiju organizacije, zaštitu imovine, funkcionalnost, ispunjavanje obaveza i zaštitu prava zaposlenih*. Bezbednosne kategorije se definišu u odnosu na ranjivosti sistema i pretnje u proceni rizika za ciljeve zaštite CIA informacija [3]. *Potencijalni uticaj* na informacionu imovinu realizuje neki agent pretnje, probojem sistema zaštite, tj. nekim gubitkom CIA. Prihvatljiva kvalitativna mera uticaja faktora rizika na objekte informacione imovine može biti: *nizak (N), srednji (S), visok (V). B*ezbednosnu kategorizaciju – **BK** svih tipova informacione imovine, određuje potencijalni uticaj gubitka ***CIA*** *(**C**=P, **I**=I, **A**=R),* koji ima *najveću vrednost*, tj. *uzima se najgori slučaj* [3]:

$$BK = \left(uticaj\ na\ P\right), \left(uticaj\ na\ I\right), \left(uticaj\ na\ R\right) = uticaj_{\max}$$

gde se vrednost potencijalnog uticaja pretnji uobičajeno rangirana sa: N, S i V.

Primer: Neka je u određivanju bezbednosne kategorije procesa *akvizicije IKTS opreme* (**BKao)** uticaj pretnji na CIA procenjen sa – (P) = **S,** (I) = **V,** a (R) = **N,** biće: **BKao**=(*P*, **S**), (*I*, **V**), (*R*, **N**) = **(S), (V), (N) = uticaj$_{max}$ = V**

Izbor minimalnog skupa kontrola za osnovnu zaštitu, uzima se iz skupa kontrola osnovne zaštite, a kontrola iz skupa za poboljšani ili viši nivo zaštite, na osnovu povećanih bezbednosnih zahteva. Na primer, ako je najveći potencijalni uticaj **N**, izaberu se osnovne kontrole zaštite za *N* uticaj pretnji, ako je **S** – izaberu se osnovne kontrole zaštite za *S* i *N* uticaj pretnji, a ako je **V** – biraju se osnovne kontrole za *V, S* i *N* uticaj pretnji. U gornjem primeru maksimalni uticaj je **V**, pa se biraju kontrole za V, S i N uticaj pretnji [25].

Prilagođavanje rezultatima procene rizika izabranog minimalnog skupa kontrola osnovne zaštite, zahteva opis i dokumentovanje modifikovanih i novih kontrola zaštite. Procena rizika igra važnu ulogu u procesu izbora kontrola zaštite, pa pokrivanje procenjenih pretnji skupom kontrola osnovne zaštite, treba razmatrati na bazi rezultata procene rizika [25].

4.4.4. Procena efektivnosti kontrola zaštite

Kontrole zaštite treba identifikovati i implementirati tako da ublažavaju specifične faktore rizika za poslovne procese. Svaka kontrola zaštite ima svoju cenu, pa zato proces njene implementacije mora uključivati tržišne faktore. Za procenu efektivnosti kontrola razvijeno je više metoda *intervjua i testiranja* (Tabela 4.4).

Tabela 4.4. Metodi za procenu efektivnosti kontrola zaštite za različite uticaje

Metodi procene: intervju, testiranje		**Nivo uticaja na IKTS**		
Atribut	**Vrednost**	**Nizak**	**Srednji**	**Visok**
Dubina (samo intervju i testiranje)	skraćen	√	–	–
	značajan	–	√	–
	sveobuhvatan	–	–	√
Obim (samo metod testiranja)	funkcionalnost (crna kutija)	√	√	√
	proboj	–	√	√
	strukturni (siv i bela kutija)	–	–	√
Pokrivanje (svi metodi)	broj i tip objekata za procenu određen u saradnji sa evaluatorom	√	√	√

U praksi zaštite treba prepoznati uslove u kojima određeni metod za procenu efektivnosti kontrola zaštite daje najbolje rezultate i ima najveću vrednost.

4.4.5. Dokumentovanje kontrola zaštite u planu zaštite

Rezultati procesa specifikacije i izbora skupa kontrola zaštite, dokumentuju se u *planu zaštite*, koji obuhvata planirane, implementirane i na bazi procene rizika, korigovane kontrole zaštite. Konačni skup kontrola dokumentuje se sa svim obrazloženjima i *glavnim razlozima* za izbor, sa indikatorima koji ukazuju na prateću dokumentaciju i koji objašnjavaju zašto izabrane kontrole ispunjavaju bezbednosne zahteve organizacije. *Plan zaštite* je osnova za sertifikaciju i akreditaciju sistema, čiji su rezultati presudni za donošenje odluke o povezivanju IKTS sa drugim sistemima izvan domena zaštite (i granica akreditacije).

4.5. REZIME

Koncept reaktivne zaštite zasniva se na sprovođenju predefinisane politike zaštite i procesu upravljanja rizikom. Sam koncept reaktivne zaštite je po svojoj prirodi proaktivan, a reaktivni karakter određuje reagovanje samo na *poznate* pretnje.

Koncept proaktivne DPP zaštite štiti sistem od dinamički promenljivih, kombinovanih pretnji, efikasniji je i efektivniji, obezbeđuje pojednostavljen, integralan sistem zaštite, reducira sve resurse, bitno poboljšava i ubrzava sveukupan proces zaštite i uspešno zamenjuje postojeće skupe, reaktivne i spore sisteme zaštite. Ostvaruje se kombinacijom *baze znanja* o novim napadima i ranjivostima sistema, *vrhunske tehnologije* za *proaktivnu zaštitu, procesnog pristupa* i *pojednostavljenog sistema zaštite* i ima tri osnovne prednosti u odnosu na reaktivni sistem zaštite: *brzinu, tačnost i pouzdanost* - manji broj lažnih alarma i veći nivo zaštite za ista finansijska ulaganja.

Koncept kontrola zaštite obezbeđuje pomoćni alat u procesu projektovanja i upravljanja sistemom zaštite, osnovne elemente za *plan* i *uputstva zaštite* i olakšava izbor optimalnih kontrola zaštite, na osnovu procene rizika. Kontrola zaštite je neka funkcija dizajna sistema koja se odnosi na *tehničke* i *proceduralne* (upravljačke i operativne) *mehanizme zaštite* i poseduju dva osnovna atributa – *robusnost* (otpornost na napade) i *adaptivnost (fleksibilnost, skalabilnost)*. *Robusnost* definiše stepen jačine bezbednosne funkcije i garantovane bezbednosti, u zavisnosti od efektivnosti implementacije, a *adaptivnost* definiše nadgradivost i izbor kontrola koje najviše zadovoljavaju definisanu politiku zaštite. Organizuju se hijerarhijski u *klase* (*U, O* i *T)*, *familije* i *kontrole zaštite*. Klasa *U kontrola* sadrži **pet**, *O* – ***devet*** i *T* – **četiri** familije. U realizaciji programa zaštite, zadatak organizacije je da definiše odgovarajući skup *kontrola osnovne zaštite*, implementira ga i verifikuje usklađenost sa *planom zaštite* i bezbednosnim zahtevima. Izbor adekvatnih kontrola demonstrira odluku za zaštitu informacija.

Sistem kontrola osnovne zaštite je minimalnih skup, koji održava ukupni preostali rizik na prihvatljivom nivou. Optimalne kontrole zaštite određuju se i biraju na bazi bezbednosne kategorizacije i klasifikacije informacione imovine i procene rizika. Svaka

modifikacija kontrola osnovne zaštite mora se dokumentovati u *planu zaštite*. Sistem kontrola osnovne zaštite za nizak (N) uticaj pretnji sadrži ukupno **198** (**U=42, O=78 i T=78**) kontrola zaštite sa niskim nivoom robusnosti.

4.6. KLJUČNI TERMINI

Fleksibilnost kontrole zaštite: omogućava izbor kontrola zaštite koje najviše odgovaraju i zadovoljavaju definisane politike zaštite i potrebe organizacije.

Koncept: osnovna zamisao, ideja, idejno rešenje, model.

Kontrola zaštite: konačna klasifikacija mehanizama zaštite, tipično neka funkcija arhitekture sistema zaštite, a odnosi se na tehničke, operativne i upravljačke mehanizme.

Operativne kontrole zaštite: uključuju organizacione i tehničke kontrole zaštite IKTS, kojima upravljaju ljudi.

Proaktivna zaštita: detekcija i sprečavanje napada od poznatih i nepoznatih pretnji/ranjivosti.

Robusnost kontrole zaštite: omogućava definisanje kontrole sa različitom jačinom funkcije zaštite u zavisnosti od efikasnosti implementacije.

Strategija proaktivne zaštite: koncept zaštite od dinamički promenljivih, kombinovanih poznatih i nepoznatih pretnji i napada.

Strategija reaktivne zaštite: koncept zaštite od poznatih pretnji i napada.

Struktura kontrola zaštite: hijerarhijska organizacija u *klase* (upravljačke, operativne, tehničke), *familije* i *kontrole* zaštite.

Tehničke kontrole zaštite: mehanizmi i protokoli zaštite, koji su implementirani i izvršavaju se unutar hardvera, softvera ili memorijskih čipova IKTS.

Upravljačke kontrole zaštite: dokumentovane mere zaštite, koje se odnose na upravljanje sistemom zaštite i procenu rizika, a izvršavaju ih uglavnom ljudi.

4.7. PITANJA ZA PONAVLJANJE

1. Koncept zaštite je:
   a. najčešće model sistema zaštite
   b. detaljna aproksimacija realnog sistema zaštite
   c. definisanje programa zaštite
   d. strategija razvoja sistema zaštite
2. Reaktivni sistemi zaštite najbolje se može predstaviti:
   a. modelom vodopada
   b. modelom sazrevanja procesa zaštite
   c. procesom upravljanja rizikom
   d. životnim ciklusom sistema
3. Ključne faze opšteg funkcionalnog modela koncepta reaktivne zaštite su:
   a. identifikacija stanja zaštićenosti sistema
   b. procena rizika, planiranje i implementaciju poboljšanih kontrola zaštite
   c. identifikacija pretnji i ranjivosti IKTS
   d. izrada politike zaštite i kontrola usaglašenosti sa praksom zaštite
   e. nadzor, revizija, obuka i obrazovanje u zaštiti
4. Koncept *proaktivne zaštite* presudno određuje:

a. manja rentabilnost vremena i troškova od postojećih reaktivnih sistema
b. reagovanje na dinamički promenljive, kombinovane pretnje
c. veća finansijska sredstva za oporavak sistema
d. detekcija i zaštita od poznatih i nepoznatih napada

5. Tipična rešenja reaktivne zaštite su:
   a. ne preduzimati ništa
   b. preduzimati redovnu kontrolu stanja bezbednosti IKTS
   c. primeniti manuelne ili polu–automatizovane metode bezbednosnih popravki
   d. izvršiti *„ad hok"* samozaštitu sa izolovanim tehničkim rešenjima na distribuiranim tačkama IKTS
6. Ključni moduli koncepta *proaktivne* zaštite su:
   a. baze znanja vodećih obaveštajnih mreža CIRT i CERT timova
   b. standardi i tehnologije za zaštitu
   c. vrhunske tehnologije za proaktivnu zaštitu
   d. procesni pristup i kompleksno rešenje sistema zaštite
   e. procesni i pojednostavljen pristup rešenju sistema zaštite
7. U sistemu proaktivne zaštite *Virtual Patch* obezbeđuje:
   a. rezervno vreme do pojave ažurne bezbednosne popravke (*update*)
   b. proaktivnu zaštitu od poznatih i nepoznatih napada
   c. slabije planiranje resursa za zaštitu
   d. bolje planiranje resursa za zaštitu
8. Sistem proaktivne zaštite ima sledeće prednosti u odnosu na reaktivni sistem:
   a. veća brzina reagovanja i tačnost detekcije napada
   b. sporija reakcija na nepoznati napad
   c. manja tačnost detekcije poznatih napada
   d. veća pouzdanost (manji broj lažnih alarma)
   e. veći nivo zaštite za ista finansijska ulaganja
9. Osnove prednosti koncepta *kontrola zaštite su:*
   a. konzistentan i ponovljiv izbor specifikacija mehanizama zaštite
   b. preporuke za *sistem osnovne zaštite* (*security baseline*)
   c. zaštita prema zahtevima bez mogućnosti proširenja
   d. tehnike i procedure za verifikaciju efikasnosti sistema zaštite
10. Pokrivanje pretnji u izabranom osnovnom sistemu zaštite mogu obezbediti:
    a. jedna kontrola zaštite
    b. kombinacija svih kontrola zaštite
    c. kombinacija određenih kontrola zaštite
    d. ni jedna kombinacija kontrola zaštite
11. *Kontrola zaštite* je između ostalog:
    a. krajnja klasifikacija servisa zaštite i neka funkcija dizajna sistema zaštite
    b. mehanizam zaštite koji se ne može kontrolisati
    c. statična i nezavisna od promena okruženja, sistema i tehnologija zaštite
    d. organizovana hijerarhijski u *familije* i *klase*
12. Familija upravljačkih kontrola zaštite obuhvata sledeće kontrole:
    a. upravljanje incidentom
    b. akvizicija sistema i servisa
    c. integritet sistema i informacija
    d. sertifikaciju i akreditaciju sistema zaštite
    e. fizička zaštita i zaštita od okruženja
13. Familija organizaciono–operativnih kontrola zaštite obuhvata sledeće kontrole:
    a. kontrola pristupa
    b. planiranje kontinuiteta poslovanja
    c. procena rizika
    d. zaštita sistema i komunikacija

14. Familija tehničkih kontrola zaštite obuhvata sledeće kontrole:
    a. planiranje sistema zaštite
    b. identifikacija i autentifikacija
    c. svesti o potrebi i obuka o zaštiti
    d. revizija i odgovornost
    e. zaštita medija
15. Sistem kontrola za visok nivo zaštite sadrži kontrole sa:
    a. osnovnim, povećanim i visokim nivoom robusnosti
    b. povećanim i visokim nivoom robusnosti
    c. osnovnim i visokim nivoom robusnosti
    d. samo visokim nivoom robusnosti
16. Bezbednosna kategorizacija informacione imovine određuje uticaj gubitka CIA koji ima:
    a. najmanju vrednost
    b. najveću vrednost
    c. srednju aritmetičku vrednost
    d. optimalnu vrednost

5. OPŠTI MODEL SERVISA ZAŠTITE

Po završetku ovog poglavlja razumećete:

- Značenje termina *servis zaštite*
- Prirodu različitih podela servisa zaštite
- Koncept opšteg, sveobuhvatnog modela servisa zaštite
- Servise zaštite u distribuiranom IKT sistemu
- Proces implementacije servisa zaštite
- Servise poverljivog provajdera zaštite (TTPS)

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET

5.1. UVOD

Implementirani skup U, O i T kontrola zaštite, izvršava funkcije i mehanizme zaštite, čijim se izvršavanjem realizuju *servisi zaštite.* Neki servisi obezbeđuju primarnu zaštitu, dok drugi otkrivaju napad ili podržavaju primarne servise. Servisi zaštite se specificiraju na osnovu zahteva i ciljeva zaštite i procene rizika.

Primarni kriterijum za podelu servisa zaštite proističe iz podele kontrola zaštite na U, O i T, na osnovu koje se i *primarni servisi zaštite* mogu podeliti na *U, O i T.* Primarne U servise zaštite realizuju U kontrole preko mehanizama prinude i nametanja normativa, standarda i politike zaštite. Operativne kontrole zaštite realizuju primarne O servise zaštite, a tehničke kontrole realizuju primarne T servise zaštite, implementacijom hardversko-softverskih mehanizama i protokola.

Ova podela nije sasvim jednoznačna, pošto su servisi zaštite međuzavisni, kombinuju se i dopunjuju u izvršavanju ciljeva i funkcija zaštite. Bolje rezultate daje opšti *model* koji prikazuje primarne servise sa elementima za podršku i njihovim međusobnim odnosima. Opšti model je više tehnički orijentisan, a deli servise zaštite na servise za *podršku, sprečavanje i oporavak.*

5.2. SERVISI ZAŠTITE

5.2.1. Misija i ciljevi sistema zaštite

Misija sistema zaštite je da održavanjem IKTS na prihvatljivom nivou rizika, obezbedi pouzdanost rada poslovnog IKTS i poveća efektivnost poslovnih procesa. *Primarni ciljevi* sistema zaštite su zaštita *CIA* informacione imovine organizacije. Ovi ciljevi se najčešće navode kao dovoljan skup relativno nezavisnih ciljeva zaštite u relevantnim standardima zaštite (ISO/IEC 27001, NIST). U nekim standardima i komponentama zaštite (evaluacija, PKI i dr.) navode se i ciljevi zaštite *kontrolisane odgovornosti* (*Accountability), neporecivosti, autentifikacije* i *garantovane bezbednosti* (*Security Assurance*). Međutim, kako su ciljevi zaštite međuzavisni, ova granulacija nije neophodna. Na primer, cilj zaštite integriteta obuhvata zaštitu neporecivosti i autentifikaciju, a cilj zaštite raspoloživosti – kontrolisanu odgovornost, koja, pak, zavisi od mehanizma za obezbeđivanje neporecivosti. Garantovanu bezbednost obezbeđuju sva tri primarna bezbednosna cilja zajedno.

Bezbednosni zahtev za raspoloživost informacija/servisa obezbeđuje ovlašćenim korisnicima pouzdan rad i raspoloživost podataka i informacija, sistema, servisa i aplikacija, po ukazanoj potrebi. Ovaj cilj štiti sistem od namernog ili slučajnog kašnjenje podataka, odbijanja izvršavanja servisa i/ili isporuke podataka (DoS/DDoS) i od neovlašćene upotrebe sistema i informacija i vrlo je često najvažniji bezbednosni cilj u mnogim organizacijama [30].

Bezbednosni zahtevi za zaštitu integriteta uključuju zaštitu integriteta *podataka i informacija* (skladištenih, procesiranih i prenošenih), *konfiguracije* (RS i RM) *i integriteta sesije*.

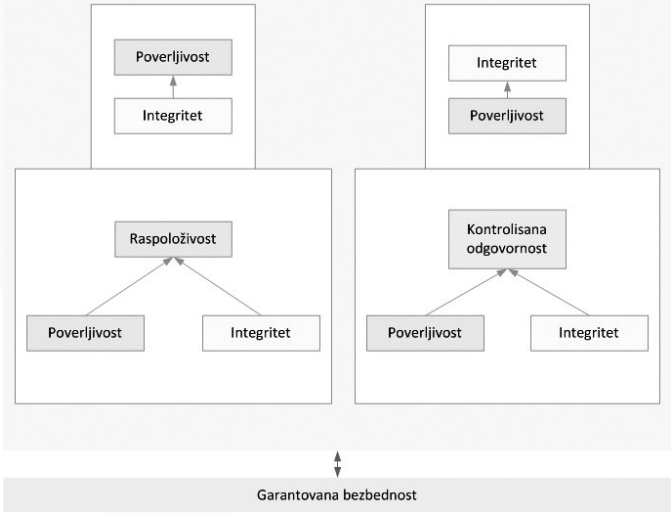
Bezbednosni zahtev za zaštita poverljivosti i privatnosti ima za cilj da spreči otkrivanje neovlašćenim licima uskladištenih, procesiranih i prenošenih poverljivih ili privatnih informacija. U sistemima za posebne namene i za specifične tipove osetljivih informacija (npr. autentifikacione), ova zaštita je od prioritetnog značaja.

Zahtev za kontrolisanu odgovornost, entiteta i pojedinca u organizaciji, ima za cilj da se akcije svakog entiteta/pojedinca mogu pratiti po jednoznačno registrovanim tragovima. Servis za ostvarivanje ovog cilja zahteva se u saopštenju politike zaštite i direktno uključuje normativni okvir, odvraćanje napadača, izolaciju grešaka, detekciju i sprečavanje upada i oporavak sistema.

Zahtev za garantovanu bezbednost sistema zaštite osnova je za sticanje poverenja da su U, O i T kontrole zaštite efektivne i pouzdano rade u predviđenom režimu. Ovaj cilj se ostvaruje adekvatnom realizacijom ciljeva zaštite *integriteta, raspoloživosti, poverljivosti* i *kontrolisane odgovornosti*.

5.2.2. Međuzavisnost bezbednosnih ciljeva

Navedeni bezbednosni ciljevi su međusobno zavisni i retko se može ostvariti jedan bez uticaja drugih. Cilj *zaštite poverljivosti* zavisi od *zaštite integriteta,* zato što nema smisla očekivati da informacija nije otkrivena, ako je narušen integritet sistema. Cilj *zaštite integriteta* zavisi od *zaštite poverljivosti,* zato što je vrlo verovatno da je mehanizam zaštite integriteta zaobiđen i integritet informacije narušen, ako je narušena njena poverljivost (npr. lozinka administratora). Ciljevi *zaštite raspoloživosti i kontrolisane odgovornosti* zavise od servisa zaštite *poverljivosti i integriteta,* zato što se mehanizmi koji implementiraju ovaj servis lako zaobilaze. Naime, ako se za određene informacije naruši poverljivost (npr. lozinka administratora), ili se naruši integritet sistema, narušava se i validnost mehanizama, koji realizuju cilj poverljivosti, a time i raspoloživosti i odgovornosti (Sl. 5.1). Svako smanjivanje ovog skupa ciljeva zahteva odgovarajuću aproksimaciju i razmatranje ove međuzavisnosti [92].

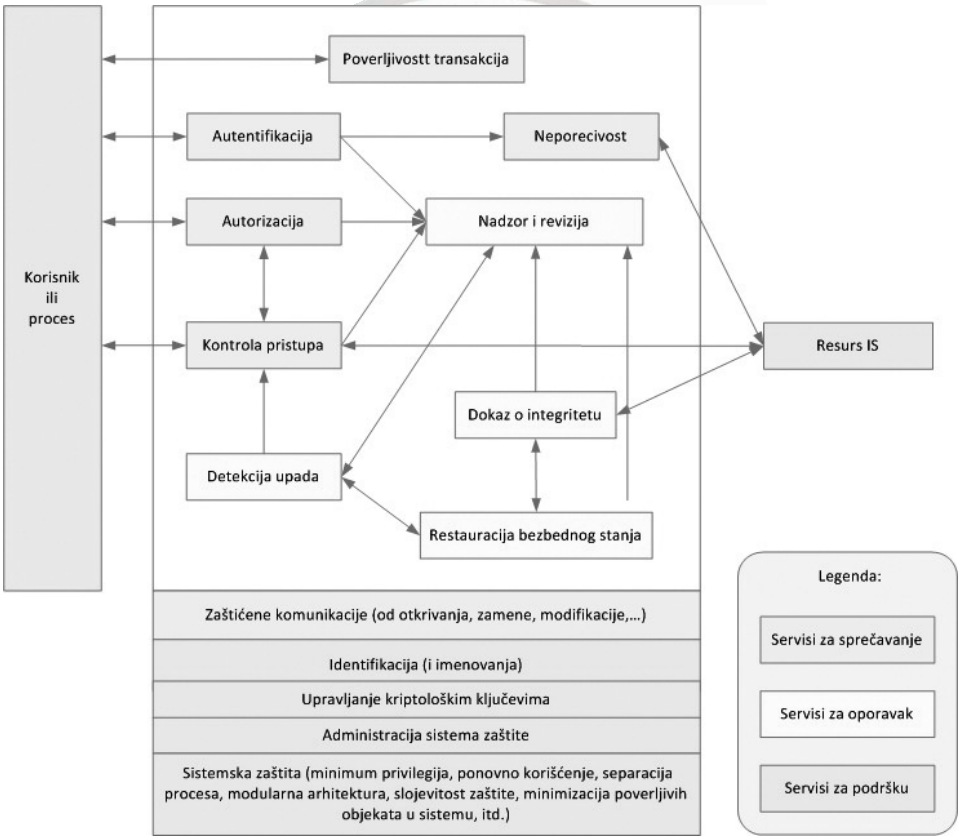


Sl. 5.1. Međuzavisnost bezbednosnih ciljeva

Sa ciljem *garantovane bezbednosti* u međuzavisnoj vezi su svi ciljevi zaštite. Kada projektuje sistem zaštite, projektant uspostavlja graničnu vrednost garantovane bezbednosti, kao cilj kojem se teži i koji se postiže ispunjavanjem zahteva u svakom od preostala četiri cilja, u skladu sa procedurama i standardima dobre prakse zaštite. Takođe, ističe činjenicu da se za garantovanu bezbednost nekog sistema moraju ispuniti projektovani funkcionalni zahtevi za *tehničku pouzdanost sistema* (verovatnoću ili srednje vreme rada bez otkaza), ali i sprečiti neželjeni procesi i steći poverenje u sistem zaštite.

5.3. OPŠTI MODEL SERVISA ZAŠTITE

Opšti model *tehnički orijentisanih* servisa zaštite obuhvata *primarne* i *sekundarne* servise i njihove međusobne veze. U odnosu na primarnu namenu, model ih klasifikuje na servise za *podršku,* koji obuhvataju najveći deo kapaciteta IKTS zaštite, *sprečavanje* proboja ili zaobilaženja mehanizama zaštite, *detekciju upada* i *oporavak* sistema posle proboja. U ovom modelu, ciljevi zaštite se realizuju servisima zaštite, pa je i njihova međuzavisnost identična međuzavisnosti ciljeva zaštite. Servisi zaštite se realizuju implementacijom hardversko-softverskih mehanizama, a izvršavaju i upravljaju sa U, O i T *kontrolama* zaštite (Sl. 5.2) [61].



Sl. 5.2. Opšti model servisa zaštite

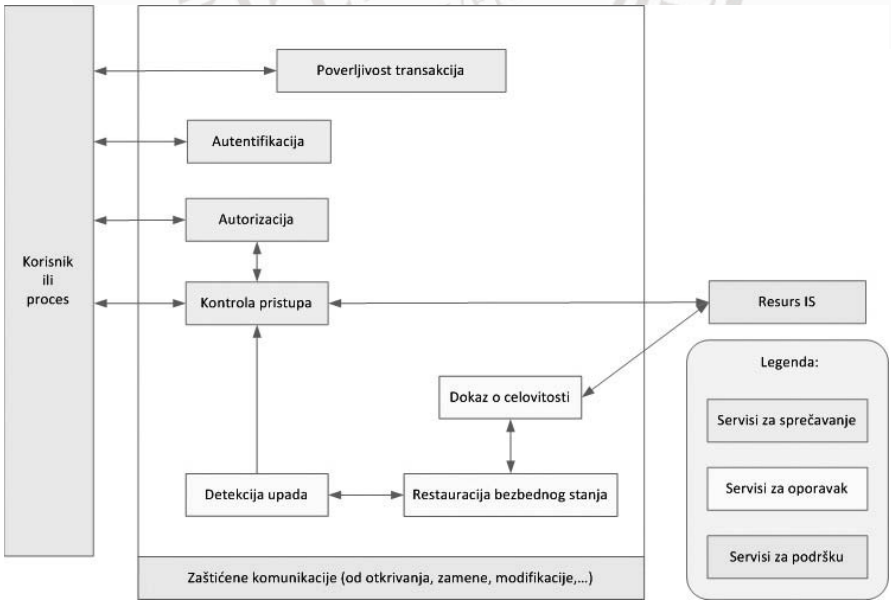
Servisi za podršku su po svojoj prirodi u korelaciji su sa drugim, obezbeđuju osnovu za poverenje u tehničke servise zaštite i obuhvataju:

- *jednoznačnu identifikaciju* entiteta (korisnika, procesa IKTS),
- upravljanje kriptografskim ključem,
- *administraciju zaštite* (operativno upravljanje promenama),
- *sistemsku zaštitu* (ponovljeno korišćenje objekata, najmanje privilegija...).

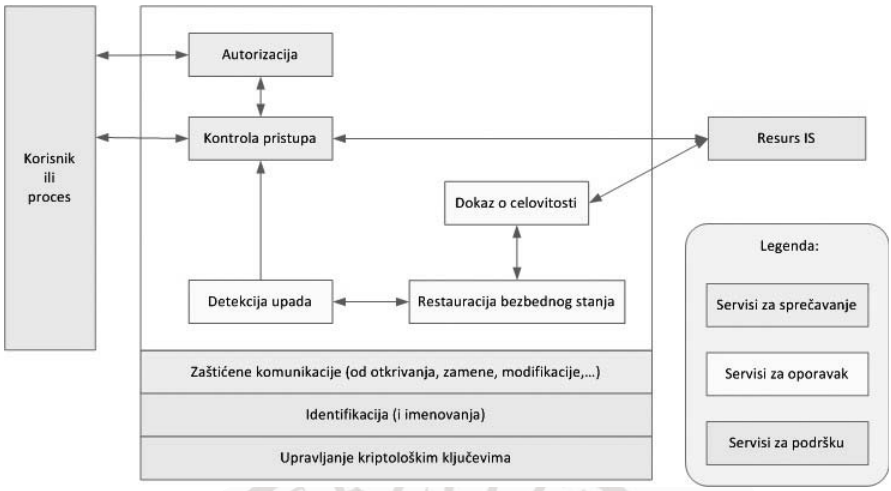
Servisi za sprečavanje preventivno štite od proboja sistema zaštite, a generički obuhvataju servise za:

- *zaštitu komunikacija,* koji štiti CIA informacija u toku prenosa,
- *autentifikaciju ili verifikaciju identiteta* korisnika i procesa u IKTS,
- *autorizaciju* prava pristupa i aktivnosti nad objektima IKTS,
- *kontrolu logičkog i fizičkog pristupa*, često distribuiranu u sistemu,
- *neporecivost,* koji sprečava da korisnik poriče izvršenu aktivnost,
- *poverljivost i privatnost transakcija,* koji sprečava gubitak poverljivosti informacija i privatnosti ličnih podataka u toku transakcije.

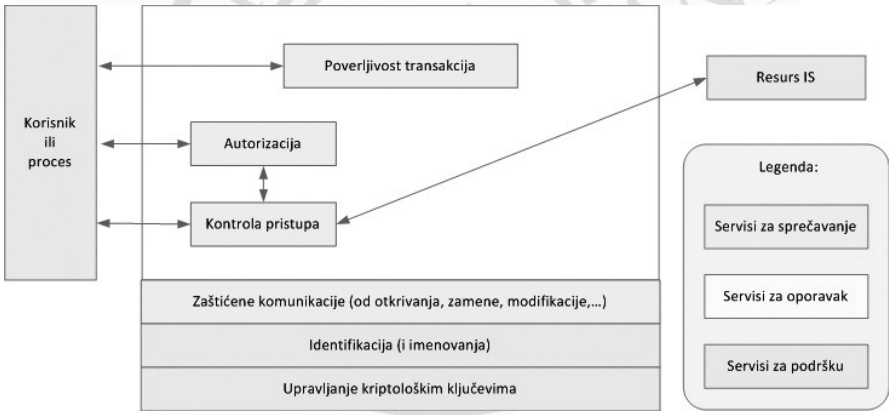
U OOM neki standardi (NIST, ISO/IEC 27001) navode minimalan i dovoljan sup od tri primarna servisa za zaštitu CIA informacija i sistema. Na slikama 5.3.–5.5. prikazani su funkcionalni modeli *primarnih servisa* za postizanje ciljeva zaštite CIA – *raspoloživosti* (Sl. 5.3), *integriteta* (Sl. 5.4) i *poverljivosti* (Sl. 5.5).



Sl. 5.3. Primarni servisi za zaštitu raspoloživosti



Sl. 5.4. Primarni servisi za zaštitu integriteta



Sl. 5.5. Primarni servisi za zaštitu poverljivosti

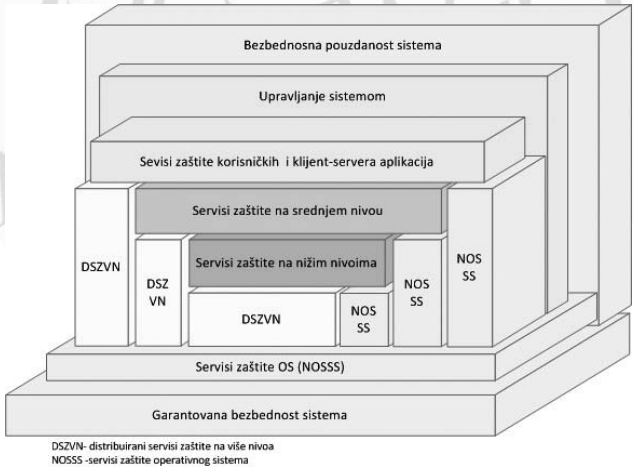
Servisi za detekciju i oporavak neophodni su u svakom sistemu zaštite, pošto ni jedan servis zaštite nije savršen, a *praktično nema sistema zaštite koji obezbeđuje apsolutnu zaštitu*. U servise za detekciju i oporavak spadaju procesi za:

- *detekciju i sprečavanje upada*, koji najčešće koriste IDPS,
- *restauraciju bezbednog stanja* ili oporavka sistema posle proboja i
- *nadzor, kontrolu i reviziju* bezbednosno relevantnih događaja.

Servisi zaštite u distribuiranom IKTS mogu biti distribuirani logički i fizički – u domenima zaštite ili u okviru fizičkih RM. Distribuirani servisi zaštite bazično zavise od tehničke pouzdanosti, garantovane bezbednosti i servisa zaštite operativnog sistema

– **NOSSS** (*Native Operation System Security Subsystem),* koji obezbeđuju osnovni sloj zaštite u RS [30, 74]. Dok neki servisi ostaju na određenom logičkom nivou apstraktnih slojeva OS, drugi su implementirani kroz mehanizme distribuirane u fizičkom i logičkim slojevima sistema: *korisničkih/klijent-server aplikacija, srednjeg sloja (midlware)* i *nižih slojeva* iznad mehanizama OS. Važan aspekat efektivnosti i efikasnosti servisa zaštite je u*pravljanje sistemom zaštite.*

Garantovana bezbednost sistema zaštite uključuje sve kapacitete zaštite i osnova je za poverenje korisnika da sistem i servisi ispunjavaju ciljeve zaštite. Poverenje korisnika u korektnost rada mehanizama zaštite i otpornost sistema na namerne ili slučajne napade, obezbeđuje kvalitetna implementacija adekvatnih kontrola zaštite. Već su razvijeni tehnološki alati za merenje garantovane bezbednosti IKTS, koja se može povećati *primenom jednostavnijih tehničkih rešenja i poverljivih i pouzdanih komponenti, smanjenjem verovatnoće proboja, implementacijom IDPS i komponenti za oporavak sistema i integracijom adekvatne tehnologije*. Na garantovanu bezbednost sistema utiče arhitektura IKTS, tzv. *zaštita bezbednom arhitekturom*. Najveću bezbednost imaju namenski sistemi, projektovani od poverljivih komponenti tzv. poverljivi računarski sistemi (*Trusted Computer Base*) [66]. Fizička i logička distribucija servisa zaštite i njihovi odnosi sa drugim servisima sistema prikazani su na Sl. 5.6. [61].



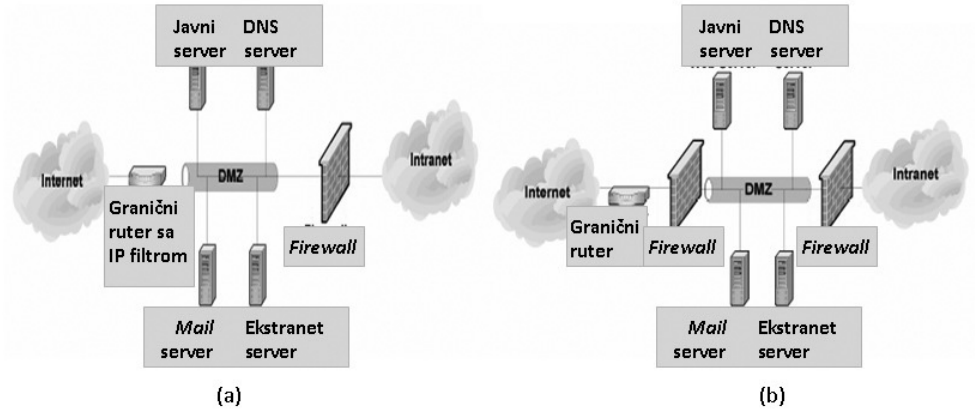
Sl. 5.6. Distribuirani servisi zaštite

Model distribuiranih servisa zaštite pokazuje da neki distribuirani servisi ne postoje individualno ni na jednom nivou, već su implementirani sa kooperativnim mehanizmima na više slojeva zaštite. Tipični primeri su servisi za identifikaciju i autentifikaciju, čiji proces obično radi na nivou OS, ali može biti na prezentacijskom, sesijskom ili čak mrežnom nivou OSI modela RM. Često se informacije skupljaju na jednoj mašini i prenose kroz RM do druge (npr. mrežni autentifikacioni i *log* serveri).

Servisi domena zaštite obezbeđuju mrežnu zaštitu i prinudnu restrikciju toka podataka i procesa unutar i između poverljivih mreža u nebezbednom Internet okruženju. *Domen zaštite je skup aktivnih entiteta (lica, procesa, uređaja), njihovih objekata podataka i međusobnih veza, koje povezuje zajednička politika zaštite*. Tipični domeni zaštite u RM sa bezbednom topologijom su *intranet, periferijska mreža* (DMZ) i *ekstranet*.

Intranet je interna mreža organizacije, koja koristi Internet tehnologije. Tipično, je fizički distribuiran i međusobno povezan uređajima, koji često nisu pod kontrolom organizacije. Interno, organizacija može podeliti intranet u relativno nezavisne module sa odvojenim *domenima zaštite*, slično vodonepropusnim vratima na pregradama broda, što pomaže da se lakše implementira politika zaštite i ograniče gubici u slučaju proboja sistema zaštite. Za segmentaciju mreže koriste se mrežne kapije (*gataways*). Postoji više rešenja segmentacije domena intraneta, koja tipično obezbeđuju *polubezbedni* domen zaštite – neutralnu tampon zonu između dve nepoverljive mreže, u kojoj organizacija može pružiti *ograničene servise* spoljnim mrežama [85].

Periferijska mreža *(zaklonjena podmreža, demilitarizovana zona* – DMZ), je *segment RM između dve mrežne barijere, koji deli mrežnu infrastrukturu na odvojene domene zaštite*. DMZ konfiguracija se može koristiti za zaštitu *web* servera mrežnom barijerom, koja dopušta pristup HTTP protokolu za *web* servise, ali ograničava sve druge protokole. Spoljna mrežna barijera štiti intranet od svakog pristupa sa Interneta, a unutrašnja sprečava odlazak zaposlenih na zabranjene *web* lokacije. Koncept domena zaštite je osnova za formiranje *bezbedne topologije* savremene RM, povezane sa Internetom – potencijalno nebezbednom mrežom. Uspostavljanje domena zaštite lokalne mreže zahteva postavljanje jedne ili više mrežnih barijera (*firewalls*). Na Sl. 5.7. prikazana je segmentacija mreže u DMZ sa jednom (a) i dve mrežne barijere (b) [85].



Sl. 5.7. DMZ sa jednom barijerom – (a) i dve barijere – (b) [85]

Domen zaštite pomaže da se odrede prioriteti zaštite, izvrši klasifikacija i usmeri pažnja na probleme zaštite, na bazi servisa koji se zahtevaju u svakom domenu. Zaštita IKTS organizacije sa DMZ i podela u domene, analogna je postavljanju fizičke ograde oko zgrade (npr. različiti tipovi barijera), kapija na ogradi (npr. *gateway*–mrežna kapija) i čuvara za kontrolu saobraćaja kroz kapije (npr. IDPS i proceduralni servisi zaštite). Domeni mogu biti logički i fizički, a definišu se na bazi jednog ili više sledećih kriterijuma: *fizički* (zgrade, kamp, region, itd.), *poslovni procesi* (personal, finansije, itd.), *mehanizmi zaštite* (OS RS, RM itd.). Ključni elementi za određivanje mehanizama, značajnih za servise zaštite u svakom domenu, su *fleksibilnost*, *projektovana zaštita*, *međusobni odnosi domena* i *slojevitost zaštite*. Različiti domeni zaštite unutar organizacije međusobno se mogu preklapati.

Ekstranet je prošireni intranet i obično se koristi za pristup udaljenih korisnika resursima intraneta i deljenje informacija i servisa. Realizuje se pomoću bezbedne *virtuelne privatne mreže* – VPN (*Virtal Private Network*) sa šifrovanom vezom, za koju su potrebna dva VPN servera ili VPN server i klijent. Pojam *eksternog okruženja* intraneta organizacije nije lako odrediti. Razlika se može napraviti između transakcija koje su istinski izvan mreže i onih koje su ekvivalentne internim transakcijama, kao što je kriptozaštićen prenos od tačke-do-tačke.

Servisi poverljivog provajdera zaštite – **TTPS** (*Trusted Third Party Services*) obezbeđuje treća strana od poverenja (TTP). Definisan je standardom ISO CD 10181-1 kao *„autoritet bezbednosti i zaštite ili njegov agent, u čije funkcije zaštite veruju svi učesnici u IKTS. Kada je TTP autoritet za zaštitu domena, može mu se verovati za zaštitu unutar domena*" [11, 61].

Standard identifikuje zahteve, koje treba da ispune korisnici i davaoci usluga (TTP), specificira i standardizuju parametre TTPS u IKTS, u kojim, osim zaštite *primarnih* servisa, treba štititi i *međusobno poverenje svih učesnika*. Tipični sistemi sa takvim zahtevima su zdravstveni, telemedicinski i savremeni sistemi e-poslovanja, u kojim se tradicionalno poverenje prenosi u nesigurno e-okruženje, kao i virtuelizovani sistemi distribuiranog Internet računarstva (*Cloud computing*), u kojima je sve više nepoverljivih korisnika [1, 11, 61, 41].

TTP servisi zaštite su obavezne komponente *višeslojne arhitekture zaštite,* posebno u sistemu distribuiranog Internet računarstva, gde odgovornosti za zaštitu servisa za isporuku softvera (*SaaS*) platformi (*PaaS*) i infrastrukture (*IaaS*) dele provajderi i korisnici na bazi SLA sporazuma. Dobar primer funkcionalnog modela TTPS je infrastruktura sa javnim ključem – PKI [11].

5.4. RAZVOJ I IMPLEMENTACIJA SERVISA ZAŠTITE

U skladu sa opštim principima i najboljom praksom, servise zaštite treba obezbediti za *životni ciklus sistema* kroz sledećih šest faza [30]:

1. *priprema* i odluka da implementacija servisa zaštite povećava efektivnost;
2. *procena* stanja sistema zaštite, identifikovanje zahteva i ciljeva zaštite;
3. *projektovanje,* razvoj i evaluacija potencijalnih rešenja iz skupa izvodljivih;
4. *implementacija* izabranih rešenja kroz pilot projekat;
5. *operativni rad* sa nadzorom, revizijom i procenom rizika i
6. *odlaganje* kroz postupnu tranzicija/ukidanje servisa zaštite.

Životni ciklus servisa primenjuje se na svaki servis pojedinačno, bez obzira u koju kategoriju spada. Implementacija servisa zaštite sopstvenim kapacitetima ili preko TTPS, može biti složena, ima svoju cenu i određeni rizik. Za donošenje odluke treba razmatrati brojna pitanja – *uticaj na strategiju i misiju organizacije, troškove, tehnologiju rada, arhitekturu IKTS, zaposlene, politiku i procese zaštite itd.*

5.4.1. Isporuka servisa zaštite

Servise zaštite isporučuje tim za upravljanje zaštitom informacija. Sistem zaštite informacija je provajder usluga za podršku poslovanja organizacije. Sa tog aspekta servisi zaštite se sastoje od tri elementa [73]:

- *isporuke* bilo kojeg proizvoda zaštite (korisnički interfejs, token, PIN, korisnički nalog, uputstvo, politika, programski kod, procena rizika itd.);
- *procesa* za održavanje kontinuiteta isporuke servisa ili skup koraka, koje organizacija treba da preduzme od prijema prve isporuke servisa zaštite;
- *merenja efektivnosti i poboljšanja* isporučenog servisa u skladu sa pravilom: *„što se ne može meriti, ne može se sa njim ni upravljati“*.

Obezbeđivanje servisa zaštite razlikuje se od isporuke fizičkih proizvoda: *nema promene vlasništva* između provajdera i kupca/korisnika, *neopipljivost* – nema razmene fizičkih objekata, *nedeljivost* – ne mogu se rascčlaniti na sitnije delove, *stalna promenljivost* – ne postoje dve identične realizacije istog servisa i *postojanost* – mogu se obezbediti samo kada njihova isporuka počne.

5.5. REZIME

Misija sistema zaštite realizuje se izvršavanjem primarnih ciljeva zaštite *CIA* informacija. Svi ciljevi zaštite su u međuzavisnoj vezi sa garantovanom bezbednosti sistema zaštite.

Podela servisa zaštite može se izvršiti na osnovu više kriterijuma. Primarni kriterijum je podela na *upravljačke, operativne i tehničke* servise. Model *tehnički orijentisanih servisa zaštite* klasifikuje servise, na osnovu kriterijuma primarne funkcionalnosti, na servise za *podršku, sprečavanje i oporavak*. *Servisi za podršku* su generički i obuhvataju najveći deo kapaciteta zaštite u IKTS; *za sprečavanje* štite od proboja ili zaobilaženja implementiranih kontrola, a *servisi za oporavak* detektuju upad i oporavljaju sistem posle proboja. Svaki sistem IKTS zaštite u krajnjem zavisi od servisa postojećih podsistema zaštite OS (NOSSS), zatim od bezbednost IKTS ne može biti veća od NOSSS. Osnova za zaštitu RM je koncept *domena zaštite* i prinudne restrikcije toka podataka i procesa unutar i između ovih domena. Domen je skup aktivnih entiteta i njihovih međusobnih veza, povezanih zajedničkom politikom zaštite. Tipični domeni zaštite su intranet, DMZ i ekstranet.

Servise zaštite može obezbediti sama organizacije ili poverljivi provajder zaštite (TTP), definisan u standardu ISO CD 10181–1. U skladu sa opštim principima i najboljom praksom, servise zaštite treba implementirati za ceo životni ciklus sistema kroz faze pripreme, procene, projektovanja, implementacije, rada i odlaganja, uz razmatranje niza pitanja o implikacijama na misiju organizacije.

Obezbeđivanje servisa zaštite razlikuje se od isporuke fizičkih proizvoda: *nema promene vlasništva*, *nisu opipljivi*, *nedeljivi su, stalno promenljivi* i *postojani u isporuci.*

5.6. KLJUČNI TERMINI

Bezbednosni cilj: definiše se na bazi zahteva za zaštitu poverljivosti, integriteta i raspoloživosti informacija.

Bezbednosni domen: skup aktivnih entiteta (lica, procesa, uređaja), njihovih objekata podataka sa zajedničkom politikom zaštite.

Bezbednosni zahtevi: zahtevi za tipove i nivoe zaštite, neophodni za opremu, podatke, informacije, aplikacije i objekte da bi se ispunile zakonske obaveze i politika zaštite.

Domen zaštite: skup elemenata kojim upravlja autoritet zaštite i koji dele istu politiku zaštite; definiše se na osnovu jednog ili više kriterijuma na fizičke i logičke domene.

Mehanizmi zaštite: pojedinačni, individualni algoritmi, metodi ili hardversko–softverski moduli za eliminisanje bezbednosnih problema u RS i mreži .

Periferijska mreža ili DMZ: segment RM između dve mrežne barijere; demilitarizovana zona/zaklonjena podmreža, koja deli mrežnu infrastrukturu na odvojene domene.

Primarni servisi zaštite: dele se na osnovu primarnih kriterijuma podele kontrola zaštite na upravljačke, operativne i tehničke servise.

Servis zaštite: skup logičkih i fizičkih aplikacija za *podršku, sprečavanje i oporavak,* koje izvršava implementirani sistem upravljačkih, operativnih i tehničkih kontrola zaštite.

TTPS (*Trusted Third Party Service):* servis poverljivog provajdera.

5.7. PITANJE ZA PONAVLJANJE

1. Misija sistema zaštite je:
   a. da održavanjem bezbednog stanja IKTS na prihvatljivom nivou rizika, obezbedi pouzdanost rada poslovnog IKTS i poveća efektivnost poslovnih procesa
   b. da omogući realizaciju politike i plana zaštite
   c. rezultat realizacije *primarnih zahteva i ciljeva* zaštite
   d. održavanje sistema zaštite na prihvatljivom nivou rizika.
2. Bezbednosni ciljevi *neporecivosti* uključuju sledeće servise zaštite:
   a. autentifikacije
   b. integriteta
   c. poverljivosti
   d. kontrolisane odgovornosti
   e. bezbednosnu garanciju
3. Bezbednosni ciljevi *autentifikacije korisnika* uključuju sledeće servise zaštite:
   a. raspoloživosti
   b. integriteta
   c. poverljivosti
   d. kontrolisane odgovornosti
   e. bezbednosne garancije
4. Bezbednosni ciljevi *integriteta* uključuju sledeće servise zaštite:
   a. raspoloživosti
   b. poverljivosti
   c. kontrolisane odgovornosti
   d. bezbednosne garancije
5. Bezbednosni ciljevi *poverljivosti* uključuju sledeće servise zaštite:
   a. raspoloživosti
   b. integriteta
   c. kontrolisane odgovornosti
   d. bezbednosne garancije
6. Bezbednosni ciljevi *kontrolisane odgovornosti* uključuju sledeće servise zaštite: raspoloživosti
   a. integriteta
   b. poverljivosti
   c. bezbednosne garancije
7. Bezbednosni ciljevi *raspoloživosti* uključuju sledeće servise zaštite:
   a. integriteta
   b. poverljivosti
   c. kontrolisane odgovornosti
   d. bezbednosne garancije
8. Ciljevi servisa zaštite *poverljivosti* i *integriteta* su:
   a. međuzavisni zato što, ako se naruši integritet sistema, narušen je mehanizam zaštite poverljivosti, a ako je poverljivost izgubljena vrlo je verovatno da će integritet biti narušen
   b. nezavisni zato što, ako se naruši integritet sistema, mehanizam zaštite poverljivosti ostaje nepromenjen
   c. cilj zaštite integriteta ne zavisi od cilja zaštite poverljivosti, ali cilj zaštite poverljivosti zavisi od zaštite integriteta
9. Servis za podršku je:
   a. namenjen za sprečavanje proboja ili zaobilaženja mehanizama zaštite
   b. namenjeni za detekciju upada i oporavak sistema posle proboja
   c. generički i obuhvata najveći deo kapaciteta IKTS zaštite
10. Servisi za sprečavanje je:
    a. namenjen za sprečavanje proboja ili zaobilaženja mehanizama zaštite
    b. namenjen za detekciju upada i oporavak sistema posle proboja
    c. generički i obuhvata najveći deo kapaciteta IKTS zaštite
11. Servisi za *detekciju i oporavak* sistema su:
    a. namenjeni za sprečavanje proboja ili zaobilaženja mehanizama zaštite
    b. namenjeni za detekciju upada i oporavak sistema posle proboja
    c. generički i obuhvata najveći deo kapaciteta IKTS zaštite
12. Servisi za *podršku* obuhvataju:
    a. jednoznačnu identifikaciju entiteta, upravljanje kriptografskim ključem, administraciju zaštite, sistemsku zaštitu

b. zaštitu komunikacija, autentifikaciju, autorizaciju, kontrolu pristupa, neporecivost, poverljivost i privatnost transakcija
c. detekciju i sprečavanje upada, restauraciju bezbednog stanja, nadzor, kontrolu i reviziju

13. Servisi za *sprečavanje* obuhvataju:
    a. jednoznačnu identifikaciju entiteta, upravljanje kriptografskim ključem, administraciju zaštite, sistemsku zaštitu
    b. zaštitu komunikacija, autentifikaciju, autorizaciju, kontrolu pristupa, neporecivost, poverljivost i privatnost transakcija
    c. detekciju i sprečavanje upada, restauraciju bezbednog stanja, nadzor, kontrolu i reviziju
14. Distribuirani servisi zaštite su:
    a. uvek implementirani na jednom apstraktnom sloju distribuiranog IKTS
    b. implementirani sa kooperativnim mehanizmima na više slojeva zaštite
    c. implementirani sa kooperativnim mehanizmima na jednom sloju zaštite
    d. bazično zavisni od tehničke pouzdanosti, garantovane bezbednosti i NOSSS
    e. nezavisni od tehničke pouzdanosti, garantovane bezbednosti i NOSSS
15. Domen zaštite, kao osnovni koncept mrež-ne zaštitu IKTS:
    a. je skup aktivnih entiteta, podataka i njihovih veza, sa istom politikom zaštite
    b. obezbeđuje mrežnu zaštitu i prinudnu restrikciju toka podataka i procesa unutar i između poverljivih mreža u nebezbednom Internet okruženju
    c. uključuje periferijsku mrežu, intranet i ekstranet
    d. ne može biti logički i fizički i ne pomaže kod određivanja prioriteta zaštite
    e. uspostavlja se primenom jedne ili više logičkih barijera (*firewalls*)
16. Glavne faze procesa za razvoj i impleme-ntaciju životnog ciklusa servisa zaštite:
    a. priprema, procena, projektovanje, implementacija, operativni rad i odlaganje
    b. planiranje, projektovanje, implementacija, operativni rad i odlaganje
    c. priprema, procena, implementacija, operativni rad i odlaganje
    d. uključuju isporuku servisa, plan isporuke i plan održavanja i odlaganja servisa
17. Glavni atributi isporučenih servisa zaštite su:
    a. servise isporučuje tim za upravljanje zaštitom informacija
    b. servise isporučuje menadžer zaštite informacija
    c. uključuju isporuku servisa, proces za održavanje kontinuiteta isporuke, merenje i poboljšanje isporučenog servisa zaštite
    d. uključuju isporuku servisa, procese za implementaciju, merenje i poboljšanje isporučenog servisa zaštite

6. METRIČKI SISTEMI ZAŠTITE INFORMACIJE

Po završetku ovog poglavlja razumećete:

- definicije «merenja», »metrike» i «metričkog sistema»
- vrste i značaj metrika u oblasti zaštite IKT sistema
- proces razvoja metrika i metričkog sistema
- metriku zrelosti procesa zaštite na bazi SSE CMM modela

6.1. UVOD

U sistemu zaštite informacija ni jedna aktivnost ne može biti dobro upravljana ako se ne može meriti. Ciljevi zaštite informacija i kvalitet sistema zaštite, mogu se postići na bazi *bezbednosnih zahteva za proizvode zaštite* (ISO/IEC 15408), *najbolje prakse zaštite* (NIST SP 800–53, ISO/IEC 27002), *procesnog pristupa i modela progresivnog sazrevanja procesa* zaštite (SSE–CMM[15]). U standardu ISO/IEC 15443 navedene su sve metode i sredstva sistema kvaliteta IKTS [46]. Razvoj metričkog sistema zaštite uključuje izbor metodologije i poznavanje i primenu generičkog procesa metričkog sistema. Pažnju zaslužuje model i metod za sazrevanja procesa zaštite – SSE CMM v. 2008.

Metrika daje svoju punu vrednost kada su merenja konzistentna, ponovljiva i bez subjektivnih kriterijuma. Kontekstualno specifična metrika je korisna u zaštiti i pomaže organizaciji da razume bezbednosni rizik i ranjivosti u infrastrukturi sistema zaštite, fokusira pažnju na tekući problem, meri i poboljšava performanse procesa zaštite i izbora najbolje tehnologije zaštite.

6.2. METODOLOGIJA METRIKE SISTEMA ZAŠTITE INFORMACIJA

6.2.1. Definicije pojmova

Merenje daje jednokratni uvid u specifične merne parametre sistema zaštite, a *metrika* je višekratno merenje u dužem vremenskom periodu ili sredstvo za interpretaciju agregiranih mernih podataka na višem nivou. Merenja se vrše poređenjem u odnosu na predefinisani merni etalon i zavisi od razumevanja zahteva zainteresovanih strana, a metrike su proizvod analize rezultata merenja. Drugim rečima, rezultati *merenja* su objektivni i sirovi podaci koji mogu automatski da se generišu, dok su *metrike* objektivne

15 Engl.: *Security System Engeneering Capability Maturity Model,* standard ISO/IEC 21827 od 2003.

ili subjektivne interpretacije tih podataka [20]. Metrika zaštite je od posebnog značaja za procese *digitalne forenzike* jer obezbeđuje *ponovljivost* testiranja i merenja digitalnih dokaza po zahtevu pravosudnih organa, što zahteva standardni kriterijum za priznavanje posrednog digitalnog dokaza pred sudom. Razni autori i standardi različito definišu *metrike zaštite* [8].

Metrički sistem je skup kriterijuma, parametara, mernih uređaja, podataka i jedinica za generisanje i prikazivanje rezultata merenja, koji podrazumeva procese *evaluacije* i/ili *monitoringa* performansi servisa zaštite. Metrički sistemi zaštite informacija su brojni, a u praksi se najčešće primenjuju: *snaga kriptografskog algoritma; kvalitativna metrika* (npr. uticaja: *nizak, srednji, visok*); *kvantitativna metrika* (*cost-benefit*); *metrika softverskog inženjerstva* (*SwE*), *detekcija anomalija* (IDS/IPS); *srednje vreme napada; intervjui; metrika poslovnih procesa; revizija sistema zaštite* i *model sazrevanja procesa zaštite (SSE CMM)*. *Objekti merenja* u sistemu zaštite informacija mogu biti *organizacija*; *proizvod* (planiran, u razvoju, u radu); *tehnički sistem* (hardver, softver, komunikaciona infrastruktura, komponente sistema zaštite, sistem zaštite u celini) [29].

Upravljanje zaštitom informacija je oblast koja nema dobro definisane metrike i još uvek ne postoji konsenzus oko ključnih indikatora, što uglavnom potiče od skrivanja bezbednosnih incidenata. Organizacije koje su imale hakerski napad, nerado to objavljuju, a one koje nisu – ne hvale se, jer ne žele da motivišu napade. Odgovorne organizacije mere aktivnosti zaštite i dokumentuju efektivnost metrika zaštite. Procesi zaštite informacija uključuju niz analitičkih ispitivanja, a odluka se lakše donosi kada postoji *metrika*.

6.2.2. Principi, namena, program i procesi metričkog sistema

Glavni principi metričkog sistema zaštite su*:*

imati obezbeđene informacije koje se mogu kvantifikovati (procenti, srednje vrednosti, gradacije 1 – 3, 1 – 5, 1 – 10),

- uvek obezbediti dostupnost podacima koji podržavaju metrički sistem,
- samo ponovljive procese smatrati merljivim,
- upotrebljiv za praćenje performansi i usmeravanje resursa za zaštite.

Namena metričkog sistema zaštite je da identifikuje uzroke slabih performansi servisa i mehanizama zaštite i omogući odgovarajuće korektivne akcije. U odnosu na **generički tip**, metrike zaštite se dele na metrike za:

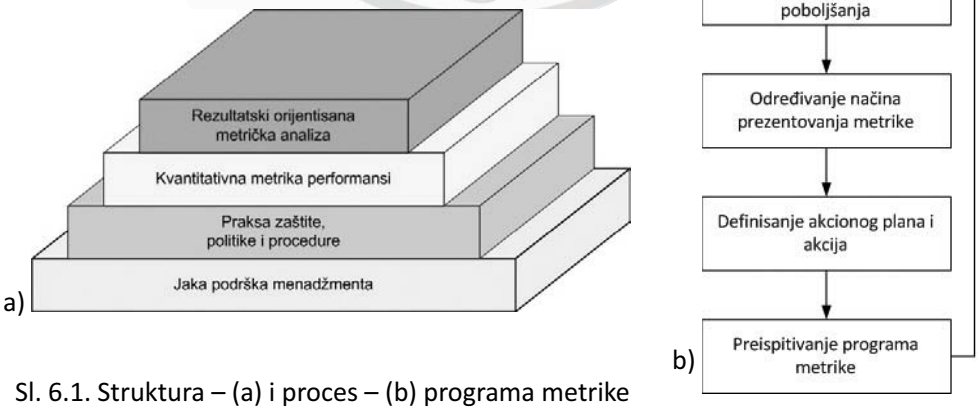
- *kvantitativno/kvalitativno vrednovanje* (proverava mehanizama zaštite) i
- *merenje performansi* (za kontinualno poboljšanje procesa zaštite).

Prvi tip metrike je *rezultatski orjentisana metrika,* a drugi – *metrika sazrevanja procesa zaštite*. Rezultatski orijentisana metrička analiza*,* bazirana na izvršavanju ciljeva zaštite, dostupna je i izvodljiva za merenje, ponovljiva i pogodna za praćenje performansi i usmeravanje resursa zaštite [40]. Rezultatski orjentisana metrika koristi se za

smanjenje troškova, povećanje prihoda, povećanje produktivnosti, smanjenje proizvodnog ciklusa i smanjenje rizika od prekida poslovanja. Metrika sazrevanja procesa zaštite vrši evaluaciju efektivnosti i poboljšavanje upravljačkih, organizacionih i tehničkih procesa zaštite i obezbeđuje relevantne podatke o izvršavanju ciljeva zaštite. Razvijeno je više metrika za merenje zrelosti procesa zaštite od kojih je samo SSE–CMM postao *de-facto* standard.

U odnosu na **objekte zaštite**, razvijena su tri tipa su *metričkih sistema* za merenje: (1) *kvaliteta implementacije politike zaštite*; (2) *efektivnosti i efikasnosti servisa zaštite* i (3) *uticaja bezbednosno relevantnih događaja na poslovanje*. Efektivnost svakog tipa metričkog sistema zavisi od zrelosti programa zaštite, organizacije i kvaliteta implementacije kontrola zaštite. Sva tri tipa metričkih sistema mogu se koristiti simultano. Sa povećanjem zrelosti implementacije kontrola zaštite, cilj je da se primarni fokus pomera sa prvog na treći tip metričkog sistem [95].

Program metrike sistema zaštite treba da uključi najmanje četiri interaktivne komponente. *Podrška menadžmenta* je kritična komponenta za uspeh programa metričkog sistema zaštite. *Politika i procedure zaštite*, neophodne su za nametanje i usaglašenost. Metrika se ne može lako izvesti, ako nema proceduru implementacije. Uspeh implementacije programa zaštite procenjuje se na bazi rezultata, pa program zaštite treba da definiše *uloge i odgovornosti za sistem kvaliteta zaštite, metrike zaštite, uputstva za merenja, metod i proces za razvoj svake metrike i faktore uticaja na implementaciju*. Program metrike zahteva periodičnu analizu za obuku, poboljšanje efektivnosti procesa zaštite i planiranje kontrola zaštite (Sl. 6.1a) [15**]**.



Sl. 6.1. Struktura – (a) i proces – (b) programa metrike zaštite informacija

Proces implementacije *programa metrike zaštite* (Sl. 6.1.b) obuhvata sedam koraka [95]: *(1) definisanje strateških i taktičkih ciljeva programa metrike, (2) izbor metrike, (3) razvoj strategije za primenu metrike, (4) uspostavljanje referentnih performansi i ciljeva poboljšanja, (5) određivanje načina prezentovanja metrike, (6) definisanje akcionog plana i akcija i (7) uspostavljanje formalnog ciklusa preispitivanja programa metrike.* Na ovaj način obezbeđuje se kontrolisan proces uspostavljanja programa metrike zaštite, konzistentnost sa ciljevima i „**kako**, **ko** i **kada"** treba da koristi njene rezultate. Ako postoji okvir za poboljšanje procesa, metrike zaštite treba da mu se prilagođavaju, a ako ne postoji – za određivanje metrike koriste se pristupi *odozgo nadole* ili *odozdo nagore* (Tabele 6.1 i 6.2). Pristup *odozgo nadole*, počinje od ciljeva programa zaštite, preko identifikovanja specifičnih metrika za određivanje stepena postizanja tih ciljeva i završava sa merenjima. Pristup *odozdo nagore* zahteva da se prvo ustanove koji su procesi, proizvodi, servisi zaštite i dr., već izmereni ili ih treba meriti, a zatim se razmatra metrika, koju je moguće izvesti iz tih merenja i određuje veza metrika sa ciljevima programa zaštite.

Tabela 6.1. Pristup za izbor metrike – *Odozgo nadole*

PRISTUP ODOZGO NADOLE	
1. Navesti ciljeve programa zaštite	**Primer ciljeva**: do kraja sledeće godine redukovati broj virusnih infekcija za 30%
2. Identifikovanje metrike za praćenje progresa svih ciljeva programa zaštite	**Primer metrike**: broj antivirusnih alarma u odnosu na presek stanja od pre dve godine
3. Odabrati merenja potrebna za svaku metriku	**Primeri merenja**: *– broj antivirusnih alarma po mesecu* *– broj prijavljenih infekcija*

Tabela 6.2. Pristup za izbor metrike – *Odozdo nagore*

PRISTUP ODOZDO NAGORE	
Identifikovati merenja za ovaj proces zaštite	**Primer merenja**: *prosečan broj detektovanih ranjivosti prvog stepena na svakom serveru po odeljenjima*
Određivanje metrike koja bi se mogla izraditi na osnovu odabranih merenja	**Primer metrike**: *promena broja kritičnih ranjivosti detektovanih na serverima od poslednjeg izveštaja o ranjivostima*
Određivanje veze između izvedenih metrika i uspostavljenih ciljeva programa zaštite	**Cilj**: *redukovati nivo detektovanih ranjivosti na serverima*

Pristup *odozgo nadole* je mnogo bolji za identifikovanje metrika, koje će biti usaglašene sa ciljevima programa zaštite, dok je pristup *odozdo nagore* lakši za određivanje metrike. Oba pristupa kreću od pretpostavke da su ciljevi programa zaštite već uspostavljeni, jer su oni preduslov za izradu programa metrike zaštite u organizacijama, koje nemaju uspostavljen okvir za upravljanje procesima zaštite.

6.2.3. Osnovne karakteristike metrika zaštite informacija

Sve metrike zaštite informacija imaju definisane neke osnovne karakteristike, (Tabela 6.3), koje omogućavaju konzistentnost primene, izbor, komparaciju i analizu, ali se u praksi, uglavnom, ne određuju.

Tabela 6.3. Karakteristike metrika zaštite informacija

Karakteristike	Komentar
Naziv	Razumljiv naslov ili naziv koji opisuje metriku
Namena	Čemu služi metrika?
Cena	Procena stvarnih troškova prikupljanja podataka za izradu metrike
Tip	Tehnička ili upravljačka, savremena ili zastarela, numerička ili tekstualna
Lokacija	Gde mogu da se prikupe podaci za metriku zaštite Gde se nalaze podaci korišćeni u prethodnim metrikama Gde su primenjene prethodne metrike zaštite
Frekvencija	Koliko često treba prikupljati podatke i prezentovati metriku zaštite
Kategorija	Broj pojave određenih događaja (**broj**); Ponavljanje događaja (**frekvencija**) Vreme utrošeno na događaj (**trajanje**); Troškovi događaja (**cena**)
Start/stop kriterijumi	Prikupljanja podataka za metriku Potrebe i prezentovanja metrike
Trajanje prikupljanja	Utvrđivanje vremenskog perioda potrebnog za prikupljanje podataka
Period upotrebe	Procena vremenskog perioda u kom će metrika biti korišćena

Najčešći primeri metrika zaštite informacija su *usklađenost sa zakonima i regulativama, demonstracija značaja zaštite informacija za organizaciju, određivanje efektivnosti kontrola zaštite, broj incidenata u datom vremenskom periodu i performanse zaštite u odnosu na budžet.* Teoretski, metrike zaštite informacija treba da daju kvantitativne, konzistentne i ponovljive rezultate i da obezbede osnovu za *analizu efektivnosti programa zaštite, izveštavanje, razumevanje načina održavanja zaštite informacija i demonstraciju vrednosti zaštite informacija za poslovanje.* Primeri metrika zaštite prema **kategorijama** dati su u Tabeli 6.4.

Tabela 6.4. Primeri metrika zaštite prema kategorijama

Kategorija	Primeri
Broj (koliko puta se nešto dogodilo)	bezbednosnih događaja; blokiranih poslovnih *e–mail;* izvršenih bekapovanja; nove informacione imovine; propusta osoblja odgovornih za zaštitu; sprečavanja korišćenja osetljivih dokumenata; sprečavanja korišćenja zaštićenih aplikacija

Kategorija	Primeri
Frekvencija (koliko često se nešto događa)	incidenata; revizije dokumenata; dodele privilegija; *udit–a* kontrole pristupa; pristupanja web lokacijama; bekapovanja servera; fizičkih pristupa server sali
Trajanje (događaja)	incidenta; bekapovanja; izloženosti pretnjama; reagovanja na incidente; pečovanja (bezbednosne popravke); oporavljanja; monitoringa
Cena (koliki su gubici zbog događaja)	rešavanja događaja ili zamene oštećene imovine; saniranja incidenta; vraćanja u prethodno stanje (oporavak); kontrola zaštite; administracije; sudskih procesa; edukacije

6.2.4. Procesno orijentisani metrički sistemi

U procesnom pristupu, razvijeno je više modela metrika sazrevanja procesa zaštite informacija [20]. SSE–CMM model sazrevanja i poboljšanja procesa i kapaciteta zaštite, obezbeđuje 6 nivoa zrelosti/kapaciteta procesa zaštite [49, 34]:

0. nivo – bez aktivnosti i izvršenih procesa zaštite (obično se u modelu izostavlja);
1. nivo – nekompletan i neformalno izvršavan, postoji politika zaštite;
2. nivo – kompletiran, dokumentovan, praćen, postoje detaljne procedure;
3. nivo – dobro definisan, implementirane i dokumentovane procedure,
4. nivo – kvantitativno meren, verifikovan, testirane usaglašenosti sa politikom;
5. nivo – kontinualno poboljšavan, potpuno implementirane u celom IKTS.

Metrika sazrevanja procesa zahteva prikupljanje i *verifikaciju* dokaza o izvršenim aktivnostima, korišćenje resursa organizacije, analizu aktivnosti sa snabdevačem, primenu metoda merenja, tačnost, ponovljivost i nezavisnost procesa itd. Za kvalitetno merenje progresivnog sazrevanja *procesa zaštite* treba definisati skup mernih atributa, za *neprekidno poboljšavanje, kvantitativno merenje i praćenje standardnih procesa organizacije, obezbeđenje podrške, planiranje i upravljanje procesima organizacije, izvršavanje i izveštavanje procesa organizacije*[32].

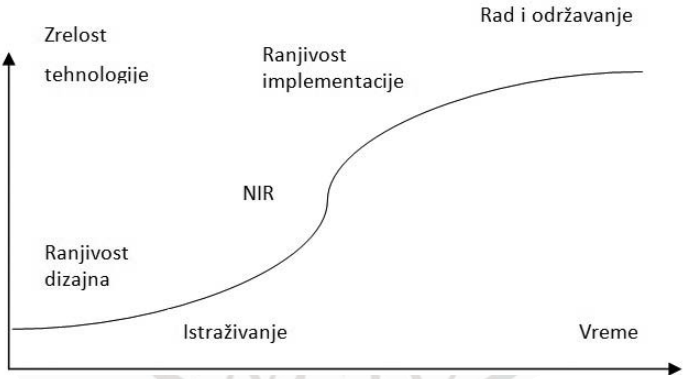
SSE CMM metrički sistem obuhvata *procesno orijentisanu metriku***,** koja se definiše sa kvantitativno/kvalitativnim dokazima o nivoima zrelosti *oblasti procesa* ili binarnom indikacijom prisustva/odsustva zrelog procesa i *rezultatski orijentisanu metriku***,** koja obezbeđuje, kao dokaze efektivnosti procesa, atribute (objektivne/subjektivne, kvalitativne/kvantitativne) rezultata merenja,.

Tehnički metrički sistemi mogu se primeniti za:

- *uspostavljanje cilja zaštite* – merenje stepena dostizanja cilja,
- *planiranje nivoa zaštite* – predviđanje nivoa zaštite pre implementacije,
- *implementirani sistem* – za merenje nivoa upada (sa IDPS),
- *usklađivanje* – merenja usklađenosti sa standardom i politikom zaštite,
- *nadzor* – skeniranje nivoa zaštite nekog objekta i za
- *analizu* – kao metod za izbacivanje grešaka.

Primeri tehničkih alata za merenje nivoa zaštite su IDPS, skeneri za monitoring mrežne zaštite, antispam i AVP, barijere i dr., koji generišu određene merne podatke i smeštaju u log datoteke zaštite. Trend je merenje zaštite iza IDPS.

Metrika proizvoda zaštite, može se primeniti u svim tačkama ranjivosti, u svim fazama životnog ciklusa (razvoja, implementacije i održavanja), zavisno od zrelosti primenjene tehnologije, koja evoluira i stabiliše se u fazi održavanja (Sl. 6.2) [88].



*Sl. 6.2. Sazrevanje tehnologija zaštit***e**

Analiza intervjua, kao metrički sistem, podrazumeva izradu *kontrolnih upitnika* (sa sedam do osam tema i oko dvadeset pitanja) o zaštiti informacija*,* intervjuisanje, skupljanje, analizu i interpretiranje rezultata, koji pokazuju *inicijalnu sliku* stvarnog stanja. Broj uzoraka za intervjue, treba biti dovoljan za uopštavanje rezultata. Oblasti za prikupljanje informacija odnose se na *kritične elemente* sistema zaštite: *U, O i T kontrole*, *organizaciju, okruženje i ciljevi zaštite, metrički sistemi (standardi i dokumentacija) i njihova implementacija, upravljanje rizikom i zaštitom itd.* [61].

6.2.5. Izbor tipa i razlozi za primenu metrika zaštite

Izbor tipa metričkog sistema zavisi od zrelosti programa zaštite. Zreo program zaštite implementira mehanizme za praćenje, dokumentovanje i kvantitativnu verifikaciju performansi sistema zaštite. Što je više podataka na raspolaganju, lakše je merenje i veća mogućnost automatizacije skupljanja podataka za kvantitativno merenje. Korisni podaci se dobiju iz automatizovanih alata za nadzor i sertifikaciju sistema zaštite, analizu baza podataka i drugih izvora. Sa aspekta zrelosti programa, razlikuju se tri tipa metričkih sistema zaštite [15, 52, 61, 40]:

1. **Tip** *(3. nivo zrelosti): procenat sistema* sa odobrenim planovima zaštite, *procenat sistema* sa politikom lozinke i pravima pristupa, konfigurisanim u skladu sa bezbednosnim zahtevima u politici zaštite. Kada merenje implementacije dostigne i ostane 100%, smatra se da su kontrole zaštite potpuno implementirane i da je sistem zaštite dostigao 3. nivo zrelosti.
2. **Tip** (*4. i 5. nivo zrelosti*): za razvijen program zaštite, podaci o performansama su dostupniji, a metrički sistem se fokusira na *efikasnost* tj. blagovremenost isporuke servisa zaštite i *efektivnost* performansi kontrola zaštite. Ova metrika je alat za *sertifikaciju* efektivnosti kontrola zaštite, npr. proračunom procenta lozinki za koje je vreme, potrebno za krekovanje, usaglašeno sa politikom zaštite lozinke.
3. **Tip** (*5. nivo zrelosti*): za kontrole zaštite, integrisane u procese organizacije, procesi postaju samo–regenerativni, a skupljanje mernih podataka potpuno automatizovano. Analizom korelacije podataka može se meriti uticaj bezbednosno relevantnih događaja na poslove i misiju organizacije. Na primer, merenje uticaja obuke, podrazumeva kvantifikovanje incidenata po tipu i korelaciju dobijenih podataka sa procentom obučenih korisnika i administratora sistema.

Rezultati istraživanja pokazuju da su osnovni razlozi za primenu metrika zaštite: *upravljanje zaštitom, usklađivanje sa zakonima i standardima, efikasnost i efektivnost performansi u odnosu na ciljeve zaštite, demonstracija značaja zaštite za organizaciju, podrška proceni rizika i upravljanju zaštitom itd.* U Tabela 6.5. date su najčešće metrike zaštite i primeri prikupljanih podataka.

Tabela 6.5. Najčešće korišćene metrike zaštite informacija

Metrika zaštite	Primeri prikupljanih podataka
Incidenti	broj incidenata u određenom periodu; uporedni prikaz broja incidenata u dva vremenska perioda; broj glavnih ili poslovno–kritičnih incidenata; cena određenog incidenta; broj identifikovanih ranjivosti; broj saniranih ranjivosti
Zaštita od virusa	broj incidenata određenog tipa virusa; broj virusnih incidenata u određenom periodu; uporedni prikaz broja virusnih incidenata u dva perioda; broj ažuriranja baze poznatih virusa; procenat uspešnih ažuriranja baza virusa; broj blokiranih virusa na *gateway*/perimetru

Metrika zaštite	Primeri prikupljanih podataka
Upravljanje rizikom	broj izvršenih analiza rizika; broj izvršenih analiza pretnji i ranjivosti; broj identifikovanih visokih/kritičnih bezbednosnih rizika; broj smanjenih visokih/kritičnih bezbednosnih rizika
Upravljanje bezbednosnim popravkama (pečevima)	broj popravljenih ranjivosti (u određenom periodu) merenje procesa (npr. izvršavanje koraka u zadatom vremenu) vreme utrošeno na popravku (npr. imovine ili kritičnih sistema) procenat popravki sistema u odnosu na SLA ili politiku procenat otkaza sistema koji nisu radili popravke
Usaglašenost sa politikom zaštite	broj izvršenih obuka za zaštitu informacija broj povreda politike zaštite
Nalazi revizije	broj neusaglašenosti otkrivenih internom kontrolom; broj neusaglašenosti otkrivenih revizijom; srednje vreme rešavanja neusaglašenosti; procenat preostalih neusaglašenosti
Troškovi	ukupni finansijski gubici zbog bezbednosnih incidenata ukupni troškovi zbog povrede regulativa ili ugovornih obaveza ukupni finansijski gubici zbog prevara (troškovi oporavka) ukupni troškovi zaštite (kontrola zaštite i posledica incidenata)

6.2.6. Primeri metričkih sistema operativnih kontrola zaštite

Za upravljanje sistemom operativnih kontrola zaštite važno je koristiti „dobru" metriku, koja treba da bude **S.M.A.R.T** [88]:

Specifična – usmerena na oblast merenja, a ne sporedni proizvod ili rezultat.

Merljiva – podaci moraju biti skupljani, tačni i kompletni.

Akciona – razumljivi merni podaci za koje je lako preduzeti akciju.

Relevantna – merenje samo onog što je važno za podatke.

T*imely* (***Blagovremena***) – podaci su dostupni kada su potrebni.

Primeri metrika koje mogu sakupiti relevantne podatke su *sistem AVP zaštite*, *upravljanje korisničkih naloga, logičke barijere, anti-spam zaštita, upravljanje web sadržaja i upravljanje politike zaštite.*

Program metričkog sistema AVP zaštite *i sistema zaštite su ključni elementi politike zaštite svake organizacije. Aplikacija merenja AVP je kritična za sprečavanje većeg uticaja na poslovanje. Centralizovano upravljanje sistemom AVP zaštite, mora imati logovanje i izveštavanje za kreiranje korisne metrike*. Za AVP zaštitu interesantno je tri do pet metrika za skupljanje podataka za analizu svake sedmice, kao što su: *broj sistema sa aktivnim AVP i ukupan broj sistema na koje treba instalirati AVP, broj sistema bez*

ažuriranih AVP definicija, broj sistema koji nisu nedavno skenirani na viruse (najmanje jedan put sedmično) i dr.

Metrika upravljanja korisničkih naloga je značajna, jer veliki broj napada dolazi iz interne mreže. Monitoring i kontrola korisničkih naloga pomaže da se spreči njihovo korišćenje za napade na IKTS. Metrika koja se može sakupiti i analizirati uključuje: *ukupan broj naloga, broj naloga koji nikad nije korišćen, broj naloga koji nije korišćen 30 ili 60 dana, broj administratorskih naloga i broj naloga servisa*.

Metrike logičke barijere su brojne i mogu se monitorisati i kontrolisati. Događaji na barijeri mogu ukazati na indikatore napada ili zloupotrebe internih konekcija IKTS. Metrika koja se može sakupiti i analizirati uključuje: *broj ovlašćenih i dezaktiviranih konekcija (po tipu), količina informacija (u MB) procesiranih po tipu konekcije i broj detektovanih obrazaca napada*.

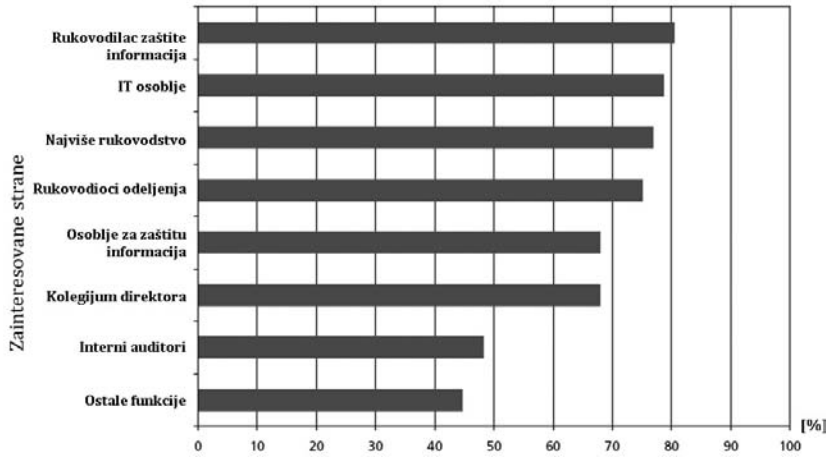
Metrike spama i integriteta sadržaja *e–mail*-a su važne u e-poslovanju, zbog porasta spama, koji sistem kontrole održava na određenom nivou i dopušta legitiman rad e–pošte. Metrika koja se može sakupiti i analizirati uključuje: *broj procesiranih poruka e–pošte, broj odbijenih poruka e–pošte zbog spama/restrikcije sadržaja, količina odbijenih poruka e–pošte u MB (propusni opseg), broj odbačenih poruka e–pošte sa neodgovarajućim sadržajem i stopa lažnih identifikacija spama*.

Metrika pristupa Internetu značajno smanjuje destrukciju rada zaposlenih i zakonske sankcije, zbog nepropisnog korišćenja Interneta, posebno sa aspekta troškova Internet opsega i gubitka produktivnosti zaposlenih. Metrika koja se može sakupiti i analizirati uključuje: *glavni akteri zloupotrebe Interneta (vreme/MB korišćenja Interneta), pokušaji pristupa zabranjenim web lokacijama, korisnička statistika vremena pretraživanja Interneta, statistika pretraživanja Interneta iz poseta web lokaciji, broj datoteka preuzetih/blokiranih /zabranjenih*.

Metrika nadzora politike zaštite je značajna za usaglašavanje svih sistema sa standardima organizacije. Aktivan program za nadzor može identifikovati sisteme koji nisu usaglašeni, a metrika može pokazati koliko je efektivna organizacija u sprečavanju/otklanjanju neusaglašenih sistema. Metrika koja se može sakupiti i analizirati uključuje: *procenat sistema usaglašenih sa standardima za zaštitu OS, lista neusaglašenih sistema i pitanja koja se moraju obuhvatiti u sistemu, verifikacija statusa popravki, procenat sistema popravljenih na zahtev*.

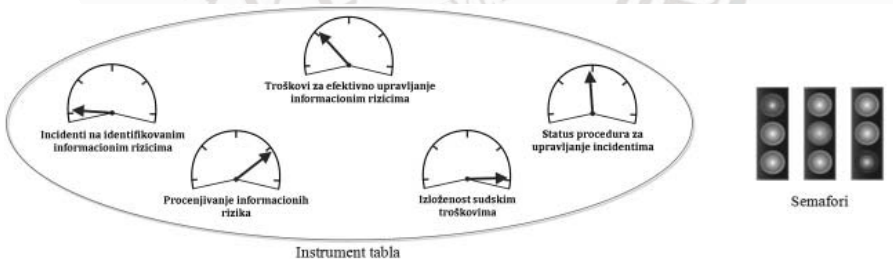
6.2.7. Prezentovanje metrika zaštite informacija

Metrike zaštite obično se prezentuju menadžeru zaštite, IKT osoblju i kolegijumu direktora, upravnom odboru ili sličnom telu u organizaciji, čime se obezbeđuje se dodatna podrška projektima zaštite informacija (Sl. 6.3).



Sl. 6.3. Uloge kojima se najčešće prezentuju metrike zaštite u organizaciji

Uobičajene forme prezentovanja rezultata metrika zaštite su *tabele sa sirovim ili statističkim podacima i analitičkim računima, semafori ili slični indikatori statusa, instrument table, tabele rezultata, grafikoni za ilustrovanje trendova ili uporedno prikazivanje rezultata i izveštaji.* Najčešće forme su *dijagrami, instrument table i izveštaji* (Sl. 6.4) [88].



Finansijski aspekt	Korisnički aspekt
• Ciljevi: o Opstanak o Uspeh/rast o Prosperitet • Merenja: o Vraćene investicije o Protok novca o Rast prihoda o Curenje kapitala o Smanjenje cena	• Ciljevi: o Akvizicija/zadržavanje/zadovoljenje korisnika o Profitabilnost • Merenja: o Zastupljenost na tržištu o Cene transakcija o Lojalnost/indeks/učešće klijenata o Odnosi sa dobavljačima o Najveći računi
Učenje i sazrevanja	**Interni poslovni procesi**
• Cinjevi: o Neprekidno unapređenje o Razvoj novih proizvoda • Merenja: o Produktivnost preduzetništva o Nove ideje/sugestije zaposlenih o Zadovoljstvo zaposlenih o Nivoi veština o Položaj osoblja o Zadržavanje zaposlenih o Profitabilnost po zaposlenom	• Ciljevi: o Ključne kompetencije o Kritične tehnologije o Poslovni procesi o Osnovne veštine • Merenja: o Efikasnost o Vreme iteracija o Pojedinačni troškovi o Godišnja stopa defekata o Vreme do tržišta

Komparativna tabela rezultata



Sl. 6.4. Primeri metoda za prezentovanje metrike zaštite informacija

Grafičke metode prezentovanja metrike, sa kvantitativnim ulazima, prenose veliku količinu informacija na jasan i sažet način. *Instrument tabla* je zgodan metod za prezentovanje rezultata menadžmentu, jer brzo i sažeto prikazuje veliku količinu podataka. Zbog celovitosti i objektivnosti, *grafikoni, semafori i tabele* najčešće se prezentuju menadžerima zaštite ili IKT osoblju. Grafikoni se često koriste za prezentovanje trendova i predviđanja. Primena jedne metode prezentovanja ne utiče jednako na sve zainteresovane strane.

6.2.8. Prednosti i nedostaci metričkih sistema zaštite

Prednosti metričkog sistema zaštite za organizaciju su brojne: *poboljšanje odgovornosti; merenje svakog aspekta sistema zaštite; izolovanje problema u zaštiti; usklađivanje sa zakonima i angažovanje na proaktivnoj zaštiti; merenje efektivnosti implementiranih kontrola zaštite* itd.

Nedostaci metrika zaštite su generalno poznati. Glavni problem je merenje uticaja ljudskog faktora na metrike zaštite, koji se delimično prevazilazi angažovanjem nezavisnih eksperata. Uzroci slabe ili neadekvatne implementacije metričkih sistema, najčešće nastaju zbog nedostatka/nepostojanja *jasno definisanih procesa metrike, svesti o potrebi upravljanja zaštitom, spremnosti menadžerske strukture za angažovanje u zaštiti, dokumenata zaštite, odgovornosti* itd. [40].

Primena metrika zaštite u praksi, najčešće je *ad hoc* proces. Ključni rezultati istraživanja primene metrika zaštite u praksi sumirani su u deset tačaka [40]:

1. Ne postoji opšta definicija metrike zaštite.
2. Metrike zaštite najčešće se odnose na usklađenost sa zakonima.
3. Najčešće se odnose na incidente, AVP, rizike, usklađenost i troškove.
4. Obično se prezentuju menadžmentu, menadžeru zaštite i IKT osoblju.
5. Mali broj metrika zaštite se odnosi na netehnička pitanja.
6. Najčešće se ne koriste za poslovne zahteve i upravljanje poslovanjem.
7. Često je teško odrediti kome i kako treba prezentovati metriku zaštite.
8. Ključni koraci programa su *definisanje zahteva, identifikovanje metrike, prikupljanje podataka i priprema prezentacija.*
9. Dobar program treba da koristi kvantitativnu i kvalitativnu metriku.
10. Prezentacija metrike treba da odgovara potrebama korisnika.

Zbog nejasne namene, metrike najčešće ne odgovaraju poslovnim ili ciljevima zaštite. Ako je loše definisan program metrike, problemi postanu vidljivi tek u fazi prezentovanja rezultata, kada se neefektivnost ne može sakriti. Osnovni problemi primene metrike zaštite otkriveni su istraživanjem modela *cilja, prikupljanja ulaznih podataka* i *način prezentovanja rezultata metrike* (Tabela 6.6) [88].

Tabela 6.6. Istraživanje primene metrika zaštite informacija u praksi

Komponente modela	Primeri iz prakse	Osnovni problemi u praksi
Zašto se koristi metrika zaštite (*cilj*)?	upravljanje zaštitom informacija izveštavanje rukovodstva usklađenost sa zakonima ... podrška upravljanju rizicima	bez jasne primene teško praćenje poslovanja nekompatibilnost sa poslovnim metrikama
Šta metrika zaštite koristi i prikuplja (*ulazni podaci*)?	incidenti, AV zaštita upravljanje rizicima upravljanje popravkama usklađenost sa politikom nalazi revizije, cena	teškoće u izboru metrike malo u poslovnoj metrici nedostatak poslovnog aspekta zaštite informacija
Kako se koriste i prezentuju metrike zaštite (*prezentacija*)?	prezentovanje raznim korisnicima razni načini prezentovanja	teško identifikovati prave korisnike težak izbor prezentovanja neprecizan opis stanja zaštite

6.3. REZIME

Metrički sistemi zaštite imaju brojne aplikacije. Ne postoje široko prihvaćeni i korišćeni standardi za merenje zaštite informacija. U oblasti zaštite metrički sistemi daju najbolje rezultate kada se primenjuju kao *proces*, planiran u pripremnoj fazi razvoja sistema zaštite. Za kvalitet programa zaštite, od presudnog značaja je razviti i implementirati program metrike zaštite, definisati proces i model ciklične evaluacije i poboljšanja procesa zaštite.

Proces razvoja metričkog sistema odvija se kroz sedam, a implementacije metrike kroz šest iterativnih koraka, koji kada se potpuno izvrše, obezbeđuju neprekidnost primene metrike zaštite za nadzor i poboljšanje performansi kontrola zaštite. Metrika zaštite je od posebnog značaja za procese *digitalne forenzike* jer obezbeđuje *ponovljivost* testiranja i merenja digitalnih dokaza.

Koncepti merenja i metrike su jasni i imaju veliku vrednost za organizaciju, jer bez merenja nema ni upravljanja zaštitom. Za efektivnu metriku aktivnosti zaštite moraju pratiti promene poslovanja, da bi ulazni podaci uvek biti aktuelni i objektivni. Najbolji način razvoja programa metrike je da se u prvoj iteraciji primeni ono što je lakše, jeftinije i što najbrže daje rezultate. Primenom komparativne tabele za prezentovanje rezultata metrike zaštite, uključujući troškovi pripreme, prikupljanja i prezentacije, biće zadovoljeni zahtevi svih zainteresovanih strana.

6.4. KLJUČNI TERMINI

Merenje: jednokratni uvid u specifične merne parametre komponente zaštite.

Metrika: višekratno merenje u dužem vremenskom periodu, ili sredstvo za interpretaciju agregiranih mernih podataka na višem nivou organizacije.

Metrički sistem: skup kriterijuma, parametara, mernih podataka i jedinica za izražavanje rezultata merenja, koji uobičajeno podrazumeva procese *evaluacije* i *nadzora* performansi servisa zaštite (tehnički sistem metrike, log datoteke).

6.5. PITANJA ZA PONAVLJANJE

1. Merenje u zaštiti informacija je:
   a. jednokratni uvid u specifične merne parametre sistema zaštite
   b. ocena opštih parametara sistema zaštite informacija
   c. vrši se poređenjem u odnosu na predefinisani merni etalon
   d. evaluacija parametara sistema zaštite informacija
   e. objektivan sirov podatak koji može automatski da se generiše
2. Metrika u zaštiti informacija je:
   a. višekratno merenje u dužem vremenskom periodu sa analizom rezultata merenja
   b. sredstvo za interpretaciju agregiranih mernih podataka na višem nivou
   c. proizvod analize rezultata merenja
   d. objektivne ili subjektivne interpretacije rezultata merenja
   e. beznačajna za proces digitalne forenzičke istrage
3. Metrički sistem je:
   a. skup kriterijuma, parametara, mernih uređaja, podataka i jedinica za prikazivanje rezultata merenja
   b. jedinica mere snage kriptografskog algoritma
   c. namenjen za ekonomsko tehničku (*cost – benefit*) analizu
   d. sistem za detekciju anomalija (IDS)
   e. SSE–CMM model sazrevanja procesa zaštite
   f. revizija sistema zaštite
4. Objekti merenja u sistemu zaštite informacija mogu biti:
   a. organizacija, informatičko odeljenje organizacije
   b. planiran proizvod, *firewall* u radu
   c. server lokalne mreže, ISP–provajder Internet usluga
   d. program glavne aplikacije, IDS/IPS
   e. mrežne komunikacije, sistem zaštite u celini
5. Glavni principi metričkog sistema zaštite su*:*
   a. ima informacije koje se mogu kvantifikovati
   b. upotrebljiv za praćenje performansi i usmeravanje politike zaštitu
   c. obezbeđena dostupnost podacima za podršku metričkog sistema
   d. samo izmereni procesi se mogu smatrati relevantnim
   e. samo ponovljivi procesi mogu se smatrati merljivim
6. Namena metričkog sistema je:
   a. identifikovati uzroke slabih performansi servisa i mehanizama zaštite
   b. omogućiti izradu plana zaštite
   c. omogućiti korektivne akcije
   d. omogućiti ponavljanje servisa zaštite
7. U odnosu na generički tip metrike zaštite se dele na metrike za:
   a. kvantitativno vrednovanje i merenje performansi procesa
   b. rezultatski orijentisanu i metriku sazrevanja procesa zaštite

c. kvantitativno i kvalitativno vrednovanje
d. kvalitativno vrednovanje i merenje performansi procesa zaštite

8. U odnosu na *objekte zaštite* razvijena su tri glavna metrička sistema za merenje:
   a. procenta sistema sa odobrenom politikom zaštite
   b. procenta implementacije sistema zaštite
   c. efektivnosti i efikasnosti servisa zaštite
   d. kvalitativne ocene incidenata
   e. kvaliteta implementacije politike zaštite
   f. stepena integracije sistema zaštite u poslovne procese organizacije
   g. uticaja bezbednosno relevantnih događaja na poslovanje
9. Ako ne postoji metrički sistem, za određivanje metrike koristi se pristup:
   a. životnog ciklusa i brzog odgovora
   b. životnog ciklusa i pristup odozgo nadole
   c. životnog ciklusa i pristup odozdo nagore
   d. odozgo nadole i odozdo nagore
10. Osnovne karakteristike metrika zaštite informacija su:
    a. naziv, namena, cena, projekat, frekvencija, kategorija, start/stop kriterijumi, trajanje prikupljanja, period upotrebe
    b. naziv, namena, cena, tip, lokacija, frekvencija, kategorija, start/stop kriterijumi, trajanje prikupljanja, period upotrebe
    c. naziv, namena, cena, tip, lokacija, frekvencija, kategorija, start/stop kriterijumi, trajanje merenja, period upotrebe
11. Glavni primeri korišćenja metrika zaštite su:
    a. upravljanje zaštitom informacija
    b. usklađivanje sa zakonima, regulativama i standardima
    c. prikazivanje efikasnosti, efektivnosti i performansi u odnosu na poslovne ciljeve
    d. demonstracija značaja zaštite informacija za organizaciju
    e. procena rizika
    f. broj incidenata u datom vremenskom periodu
    g. ukazivanje na prednosti i nedostatke standarda zaštite
12. Glavne faze generičkog toka procesa uspostavljanja programa metrike zaštite su:
    a. uspostavljanje referentnih performansi i ciljeva poboljšanja
    b. izbor i razvoj strategije za primenu metrike
    c. uspostavljanje referentnih performansi i ciljeva merenja
    d. razvoj i preispitivanje tehnike merenja
    e. izbor načine prezentovanja tehnike merenja
    f. definisanje akcionog plana izbora metrike
13. Glavne komponente strukture programa metrike zaštite su:
    a. praksa, politika i procedure zaštite
    b. metrika sazrevanja procesa zaštite
    c. podrška menadžmenta
    d. kvalitativna metrika performansi
    e. rezultatski orijentisana metrička analiza
    f. kvantitativna metrika performansi
14. Za procesno orijentisani sistem sazrevanja procesa zaštite treba definisati atribute za:
    a. neprekidno poboljšavanje, podršku, planiranje i upravljanje procesima organizacije, izvršavanje i izveštavanje
    b. neprekidno poboljšavanje, praćenje procesa zaštite, podršku, planiranje i upravljanje procesima zaštite, izvršavanje i izveštavanje
    c. neprekidno poboljšavanje, kvantitativno merenje i praćenje procesa zaštite, podršku, planiranje, izvršavanje i izveštavanje procesa zaštite
    d. neprekidno poboljšavanje, kvantitativno merenje i praćenje procesa zaštite, podršku i planiranje, izvršavanje i izveštavanje

15. Sa aspekta zrelosti programa razlikuju se tri tipa metričkih sistema zaštite:
    a. procenat sistema sa odobrenom politikom lozinki, efikasnost i efektivnost performansi kontrola zaštite, uticaj bezbednosnih događaja na poslovanje i misiju
    b. procenat sistema sa odobrenim planom/politikom, efikasnost i efektivnost performansi kontrola zaštite, uticaj bezbednosnih događaja na poslove i misiju
    c. procenat sistema sa odobrenim planom zaštite, efikasnost i efektivnost poslovnih procesa, uticaj bezbednosnih događaja na poslove i misiju organizacije
16. Najčešće korišćene metrike zaštite su za:
    a. praćenje incidenata, zaštitu od virusa, upravljanje bezbednosnim popravkama, merenje usaglašenosti, reviziju i troškove zaštite
    b. praćenje incidenata, zaštita od virusa, merenje usaglašenosti i reviziju
    c. zaštitu od virusa, upravljanje bezbednosnim popravkama, merenje usaglašenosti
    d. troškove zaštite, zaštitu od virusa, upravljanje bezbednosnim popravkama
17. Tipične kategorije parametara za metriku zaštite uključuju:
    a. veličinu, frekvenciju, trajanje i cenu
    b. broj, frekvenciju, trajanje i cenu
    c. broj, veličinu, frekvenciju, kvalitet servisa, trajanje i cenu
18. Tehnički metrički sistemi se mogu primeniti za:
    a. uspostavljanje cilja zaštite, implementirani sistem, usklađivanje, nadzor i analizu
    b. uspostavljanje cilja zaštite, planiranje nivoa zaštite, implementirani sistem, usklađivanje, nadzor i analizu
    c. planiranje rizika, implementirani sistem, usklađivanje, nadzor i analizu

7. TAKSONOMIJE PRETNJI I MALICIOZNIH PROGRAMA

Po završetku ovog poglavlja razumećete:

- značaj taksonomija pretnji
- osnovne tipove malicioznih napada (virusi, crvi, trojanci,...)
- mere zaštite i oporavka sistema od malicioznih napada

7.1. UVOD

Uporedo sa razvojem Interneta, rastu i potencijalne pretnje spolja i iznutra. *Intranet* mreže nude brojne prednosti (povećanje produktivnosti, smanjenje troškova itd.), ali čine i kritičnu tačku bezbednosti za CIA informacija. Istraživanja pokazuju da mnogo veću štetu nanose interni napadi u sistemu e-poslovanja, u kojima interni korisnici nisu samo zaposleni za koje postoji određeni stepen poverenja, već i brojni spoljni saradnici, koji imaju vrlo sličan pristup intranetu.

Pored finansijske dobiti, brojni su motivi za razne vrste namernih napada, među kojima su najčešće izazov i potreba za samopotvrđivanjem, znatiželja i maliciozne namere – krađa i oštećenja informacija, špijunaža informacija itd.

Mogući načini odbrane od navedenih napada su slojevita antivirusna, šifrovanje, procedure jake autentifikacije i korišćenje *smart* kartica za generisanje digitalnog potpisa i bezbedno čuvanje ključeva kriptografskih parametara za jaku autentifikaciju, primena tehnologije digitalnog potpisa, korišćenje i česta izmena jakih ključeva, zaštita IP adresa servera i dr. Najbolje rezultate daju kombinovani sistemi višeslojne zaštite po dubini, na bazi analize rizika.

7.2. PRETNJE I NAPADI

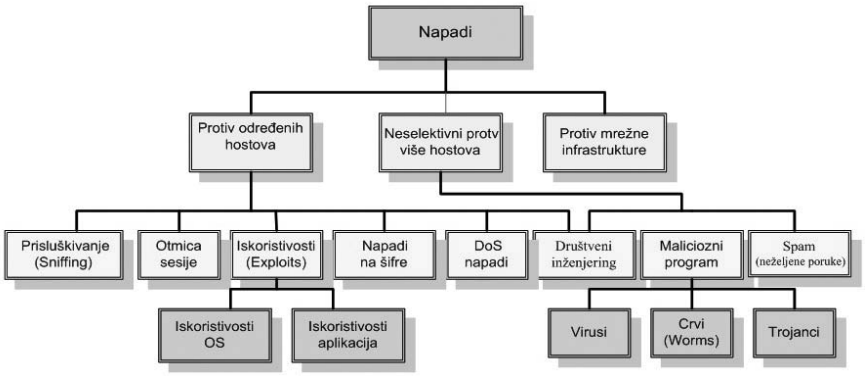
7.2.1. Taksonomije pretnji i napada

Moguće su brojne *taksonomije*[16] *agenata pretnji*. Krajnji cilj svake taksonomije pretnji je da specijalisti zaštite i korisnici lakše definišu i identifikuju različite tipova promenljivih pretnji za IKTS**.** *Taksonomija izvora pretnji* deli pretnje na *slučajne* – Sl i *namerne* – Na. Slučajne su nenamerne ljudske greške, otkazi hardvera i softvera, prirodni vanredni

16 Taksonomija (engl. *taxonomy*) - principi i teorija klasifikacije na bazi strogo definisanih kriterijuma.

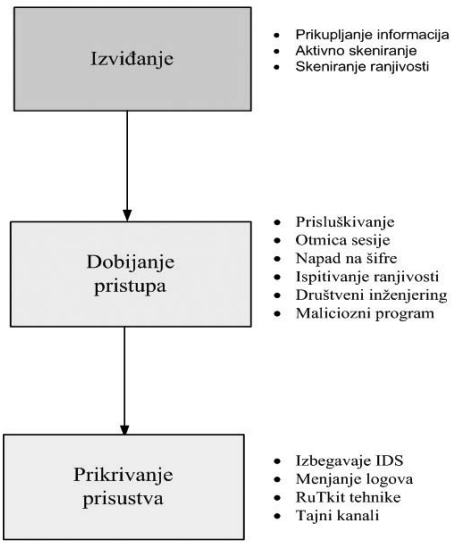
događaji itd., a namerne pretnje generišu ljudi. Za upravljanje rizikom od interesa je procena svih pretnji koje izazivaju bezbednosne incidente. Na osnovu ove podele, pretnje se klasifikuju u 6 kategorija [32, 63, 94, 79, 97]: *(1) maliciozne zloupotrebe ranjivosti IKTS, (2) kompjuterski kriminal,* (3) n*ebriga*, (4) *ljudska greška*, (5) p*ad sistema* i (6) u*ticaj okruženja*.

Realizovana pretnja u IKTS naziva se *napad*, koji može biti *uspešan* ili *neuspešan*, zavisno od jačine napada i otpornosti sistema zaštite. Generička taksonomija napada prikazana je na Sl. 7.1.



Sl. 7.1. Generička taksonomija napada

Napadi se često vrše kroz progresivne korake, analogno fizičkom napadu (Sl. 7.2). Prvi korak je izviđanje i prikupljanje informacija, zatim, skeniranje ranjivosti sistema, što je od kritičnog značaja za uspeh napada. Drugi korak je dobijanje pristupa, koji može imati različite ciljeve, kao što su kontrola, krađa ili uništenje podataka.



Sl. 7.2. Generički tok napada na računarske mreže i sisteme

Taksonomija kombinovanih napada prihvatljiva je za *kvalitativnu analizu rizika* u odnosu na sledeća tri kriterijuma: **(1) posledica uticaja**: štetan **– Št,** neškodljiv **– Nš; (2) izvor nastanka**: iznutra – **Un,** spolja – **Va** i **(3) način izvođenja:** sofisticiran

– **So,** nesofisticiran – **Ns**. U praksi se ovi napadi najčešće realizuju u kombinaciji i proizvode uticaj na informacionu imovinu kroz osam kombinacija [91]:

$$\left(\check{S}_t S_o U_n,\ \check{S}_t SoVa,\ \check{S}_t N_s U_n,\ \check{S}_t N_s V_a,\ N_{\check{s}} S_o U_n,\ N_{\check{s}} S_o V_a,\ N_{\check{s}} N_s U_n,\ N_{\check{s}} N_s V_a\right)$$

Redukovana taksonomija izvora pretnji za izbor *kontrola* zaštite, klasifikuje izvore pretnji na *greške, prirodne događaje i namerne napade,* obično maliciozne sa promenljivim stepenom intenziteta, zavisno od *tipa, sposobnosti, resursa, motivacije, prilike i namere napadača* **(**Tabela 7.1) [91].

Tabela 7.1. Zbirne karakteristike atributa namernih napada

TIP NAPADA	
Lokalni	zahteva se fizičko prisustvo napadača na mestu napada i razmeštaja IKTS
Mrežni	napadač inicira napad sa mreže
SPOSOBNOST NAPADAČA	
Niska	uobičajene sposobnosti i ograničeno znanje o IKTS i ne koristi posebne alate
Visoka	ima jednu/obe sposobnosti: koristi sofisticirane alate i/ili napredne IKT tehnike
PRISTUP IS	
Iznutra	napadač nije korisnik, nije privilegovan korisnik ili je privilegovan korisnik IKTS
Izvana	napadač je legalan ili nelegalan ili javni korisnik IKTS
NAMERA NAPADAČA	
Nemaliciozan	nema nameru da ošteti IKTS, napada iz znatiželje, dosade ili izazova
Maliciozan	ima jasnu nameru da ošteti IKTS, ili izazove štetu organizaciji
RESURSI NAPADAČA	
Minimalni	(I) samoinicijativan i samo–motivisan; (II) radi nezavisno i (III) izvršava napad sa minimalnim računarskim resursima
Srednji	(I) deo grupe/organizacije, koje se ne bave komercijalnom špijunažom, kriminalom, ili terorizmom); (II) radi pod uticajem grupe/organizacije i (III) izvršava napad sa prosečnim resursima
Značajni	(I) deo grupe/organizacije, uključujući obaveštajne, informacionog ratovanja ili državno–sponzorisanog terorizma; (II) radi direktno pod upravom grupe/organizacije i (III) napada sa značajnim resursima

Ključni tipovi napada mogu se svrstati u sledeće grupe: *destrukcija, izmena podataka, prekid servisa (DoS, DDoS*[17]*), špijunaža i neovlašćeno korišćenje* [91].

Opšti motivi napadača – *hakera, krakera, vandala, kompjuterskih kriminalaca i* dr su znatiželja, novac, moć, osveta i sl. Od *posebnih motiva* presudni su intelektualni izazov, radoznalost, avanturizam, zabava, potreba za trijumfom, opijenost sopstvenim znanjem, kompenzacija osećaja manje vrednosti, osećaj elitizma, pritisak hakerske organizacije, prestiž i dr. Hakeri se prema kriterijumu *namere* mogu podeliti na *kreativce, destruktivce i kriminalce.* Kreativci najčešće ne prave štetu, dok je destruktivci prave – uništavaju, brišu i menjaju podatke. Kriminalac je tipično mlad, inteligentan, uzoran i odgovoran radnik na poslu, spreman na prekovremeni rad, visoko motivisan i istraživački orijentisan. Ima razvijeno logičko mišljenje, dobro poznaje i koristi RS, samo mu treba jak motiv, da postane pohlepan, osvetoljubiv i sl. *Sredstva* za napad čine tehnički kapaciteti i nivo veštine koju hakeri poseduju. *Prilika* za napad je iskoristiva ranjivost, koja se teško određuje zbog mogućnosti postavljanja raznih zamki (zadnjih vrata, trojanaca,...).

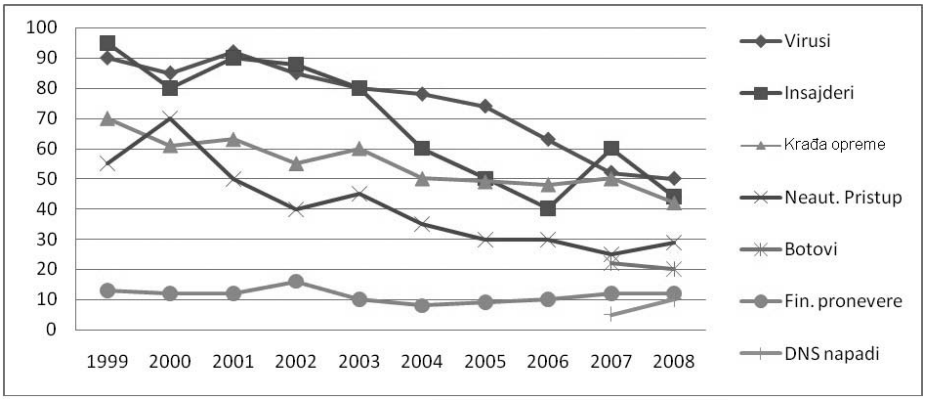
Napadi mogu biti usmereni na *određene hostove* (prisluškivanje, otmica sesija, skeniranje ranjivosti, probijanje lozinki, odbijanje servisa i društveni inženjering), infrastrukturu RM ili nasumice prema hostovima. Društveni inženjering se može koristiti za masovne neselektivne napade – *spam* (neželjene poruke) i slanje ili ubacivanje malicioznog koda. Vektor napada poslednjih godina pomera se sa relativno dobro zaštićenih servera lokalnih mreža, na *web* servere, baze podataka na *web*–u i pojedinačne nezaštićene računare umrežene na Internet (Tabela 7.2).

Tabela 7.2. Pomeranje vektora napada sa Interneta

1996. godine	**2009/2010. godine**
Hakeri iz hobija	Profesionalni hakerski napadi na *web* servise
Prevaranti na *web* sajtovima	Organizovani kompjuterski kriminalci
Virusi i drugi maliciozni programi	Napadi odbijanja servisa (DoS, DDoS)
Retki napadi na *web* servere	Krađa identiteta, iznuđivanje, ucene
	Stalni napadi na *web* servere i društvene mreže

U toku 2008. godine broj malicioznih programa u opticaju [104] iznosio je preko milion, od kojih je većina i kreirana iste godine [96]. U 2008. godini preko 50% svih napada na IKTS organizacija činili su virusi i napadi iznutra koji su u opadanju, ali i dalje najčešći uzrok kompjuterskog incidenta, (Sl. 7.3) [96].

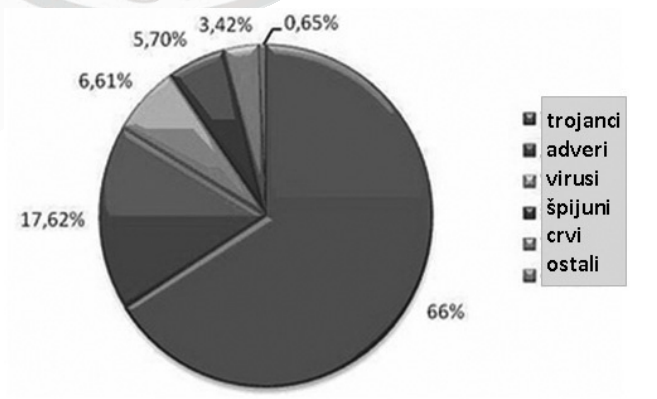
17 *Dinail of Services/Distributed Dinail of Services* – odbijanje/distribuirano odbijanje izvršavanja servisa.



Sl. 7.3. Ključni tipovi incidenata izraženi u procentima (2008.) [96]

U 2008. godini *Oracle* je identifikovao **osam** sigurnih načina za hakerisanje *Oracle web* baza podataka. Tipičan metod hakerskog napada čine faze *pripreme i planiranja*, *izbor cilja* (sakupljanje informacija), *planiranje napada*, *izbor metoda/tehnike napada* (rutkit, trojanac, brisanje podataka...) i *izbor mera* samozaštite. Glavne tehnike za napad su *rutkit tehnike* koji prikrivaju prisustvo u računarskom sistemu i postavljanje zadnjih vrata za kasniji ulazak u sistem. Samo u 2009. godini registrovano je 25 miliona novih malicioznih programa [103], od čega čak 66% novih tipova trojanaca za krađu novca iz banaka, kao i lažnih, malicioznih AVP (Sl. 7.4). Troškovi zloupotrebe IKTS definišu se kao: *potreban rad da se analizira, popravi i očisti inficirani sistem ili gubitak produktivnosti i drugi troškovi otklanjanja posledica napada*, koji ne uključuju preventivnu zaštitu (nabavku AVP, obuku, troškove osiguranja i troškove gubitka ugleda) [96].

Rezultati istraživanja finansijskih aspekata zloupotrebe IKTS (*Computer Economics,* 2007.), pokazuju da su za deset godina (1997 – 2007) porasli sa 3,3 mlrd$ na 13,3 mlrd$ [96]. Napadi malicioznim programima neprekidno rastu, a štetne posledice se menjaju iz godine u godinu, od jedne do druge statističke analize. Anti–virusna kompanija *Panda Security Labs* je 2009. godinu objavila da je od januara – avgusta 2008. detektovala više podvrsta malicioznog softvera nego u prethodnih 17 godina [96]. Očekuje se i povećan



Sl. 7.4. Zastupljenost malicioznih napada u 2009. [96]

broj malicioznih programa koji napadaju nove operativne sisteme *Leopard, Windows 7* i *Ubuntu* [96]. U toku 2009. svakog dana na Internetu javljalo se prosečno 37.000 novih tipova malicioznih programa (*malware*) i napada, od kojih je njih 40% menjalo svoju definiciju u prva 24 časa [96]. U prvoj polovini 2010. godine, maliciozni programi na Internetu su premašili po broju svaku polugodišnju produkciju do sada. Procene su da se dnevno generiše oko 63.000 novih, od kojih preovlađuju *AutoRun* i *trojanac* koji krade lozinke [96]. Istovremeno *spam* je dostigao najviši nivo u treće, kvartalu 2009. – 175 milijardi *spam* poruka. Tipovi *spama* variraju u različitim državama. Notifikacija statusa isporuke ili prihvatanje neisporuke *spama* (*non–delivery receipt spam*) najviše se koriste u SAD, Italiji, Španiji, Kini, Brazilu i Australiji. Maliciozni *spam* ili sve što stiže sa prilogom, koji unosi virus ili trojanca, najšire su zastupljeni u Kolumbiji, Indiji, Južnoj Koreji, Rusiji i Vijetnamu. U Argentini ima šesnaest tipova spama, a u Italiji – samo šest. Takođe, ponovo su oživele dve najveće botnet mreže na svetu – *Storm Worm i Kraken*. U **Prilogu 5.** data je kratka istorija razvoja malicioznih programa.

7.3. PREGLED MALICIOZNIH PROGRAMA

Uvođenje malicioznih programa sa Interneta smatra se konstantnom pretnjom za IKTS. Maliciozni program je kôd koji se tajno ubacuje u drugi program sa namerom da se nanese šteta, unište podaci, pokrenu destruktivni programi ili kompromituje bezbednost informacija. Pod štetom se podrazumeva svako ometanje normalnog funkcionisanja IKTS i procesa koje podržava. Malicioznost je određena namenom, a ne algoritmom ponašanja kôda. Na primer, crv *W32.Welchia* se ponaša i izgleda kao maliciozni kôd, a zapravo preuzima poslednje *Microsoft* popravke i uklanja crv *W32.Blaster*. Granice između raznih malicioznih kôdova su sve slabije. Najopasnija je sprega lažnih virusa (*hoaxes*) i trojanaca, jer ne inficira sistem, uporna je, teško se otklanja, a distribuira viruse i trojance [96].

Virusom, crvom i trojancem, sistem se može zaraziti na više načina – preko USB, CD, DVD i sl.; priloga e–pošte ili preuzetog sadržaja sa Interneta; *web* lokacije sa instaliranim virusom ili skriptom koji generiše viruse ili trojance; iskorišćavanjem ranjivosti sistema itd.

7.3.1. Osnovne vrste savremenih malicioznih programa

Maliciozni kôdovi mogu uticati na sve aspekte zaštite. Najčešće se prema vrsti napada ili funkcionalnosti dele na *viruse, crve, trojance, mobilne kôdove i kombinovane napade*. Ranije je ovakva podela bila moguća, ali su ovi programi evoluirali i često kombinuju više funkcionalnosti. U Tabeli 7.3. dati su osnovni kriterijumi klasične podele malicioznih programa *umnožavanje, samorazvoj i parazitnost* [111].

Tabela 7.3. Uporedne karakteristike nekih malicioznih programa

Maliciozni kôd	Umnožavanje	Samorazvoj	Parazitnost
Virus	da	da	da
Crv	da	da	ne
Trojanac	ne	ne	da
Backdoor	ne	ne	moguće
Spyware	ne	ne	ne
Logička bomba	ne	ne	moguće

7.3.2. Taksonomija virusa

Od brojnih definicija virusa najčešće se koristi prva[18]: „*Računarski virus* je *program koji ˝inficira˝ ostale programe, modifikujući ih tako da uključuju njegovu naprednu kopiju*. *Sa inficiranog područja, virus se može širiti kroz RS i RM, koristeći autorizaciju svakog korisnika da inficira njihove programe. Svaki program koji se inficira, takođe se ponaša kao virus pa se infekcija povećava*“. „*Računarski virus je segment mašinskog kôda, obično od 200–4000 bajta, koji će nakon aktiviranja kopirati svoj kôd na jedan ili više programa domaćina. Izvršavanjem programa domaćina, izvršava se „inficirani“ kôd i virus nastavlja da se širi.*“ [19].

Računarski virus je dizajniran da se replicira, pravi svoje kopije i distribuira ih u druge datoteke, programe ili računare sa ciljem da napravi štetu. Širi se uglavnom tako što se *ugnezdi* u drugu datoteku, a zatim je briše ili menja. Virus iz inficiranog računara u RM traži drugi računar da ga zarazi[20].

Viruse generišu gotovo isključivo tehnički virtuozi radi *malicioznih namera*, *komercijalne dobiti* i *hakerskog ratovanja*. Generalno, svi virusi su maliciozni, pošto i tzv. benigni, iako nisu štetni, zauzimaju resurse računara i vrše neželjene radnje. U principu, bilo koji program može prenositi viruse, ali je to najčešće program namenjen za veći broj korisnika. Neki virusi napadaju samo određene, dok drugi napadaju više programa. *Taksonomije virusa* su brojne, a broj virusa u stalnom porastu. Česta klasifikacija je na viruse *BOOT sektora, komandnog procesora, univerzalne infektore datoteka, usmerene, makro i lažne viruse*[21].

Virusi BOOT sektora *kače* se uz *master boot record* (MBR) u *boot* sektoru čvrstog diska (HD), jedinstvenoj lokaciji na HD, gde su smešteni osnovni ulazno/izlazni sistem (BIOS) računara i program za podizanje OS. Ako je HD *inficiran u drajveru*, virus se može

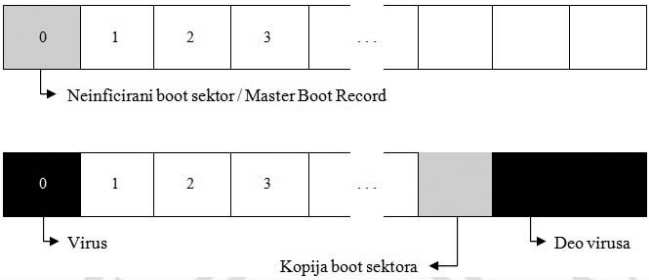
18 Fred Cohen, *Computer Viruses: Theory and Experiments*, Fred Cohen & Associates, 1984.

19 Aycock John, *Computer Viruses and Malware,* Springer, 2006.

20 Jakobsson Markus, Zulfikar Ramzan, *Crimeware: Understanding New Attacks and Defenses,* Addison Wesley Professional, 2008.

21 Mell, P., Kent, K., Nusbaum, J., *Guide to Malware Incident Prevention and Handling*, Special Publication 800-83, Novembar 2005.

aktivirati pre bilo kojeg dela OS, kada se računar podiže. Ovi virusi se nalaze u najdubljem delu OS, mogu preuzeti kontrolu i nadgledati svaku operaciju, a pokreću se pre AVP i na taj se način uspešno kriju. Uklanjaju se jedino reinstalacijom OS sa originalnog *butabilnog* CD, zaštićenog od snimanja, uz paralelnu upotrebu AVP. Ovi virusi su jednostavni za kreiranje, relativno dobro sakriveni (ako ne prikazuju poruke na ekranu), ali se lako odstranjuju. Danas su retki zbog hardverske zaštite i autorizacije da bi se moglo upisivati u *boot* blok (Sl. 7.5). Klasični primeri ovih virusa su *Michelangelo* i *Stoned*.



Sl. 7.5. Prikaz neinficiranog i inficiranog boot sektora

Virusi komandnog procesa slični su prethodnim, osim što se učitavaju malo kasnije u procesu podizanja OS. Njihova moć nad OS je samim tim manja. Kada se otkriju, lako se uništavaju.

Univerzalni virusi infektori datoteka su najširа kategorija virusa, pored virusa *boot* sektora i MBR. Najčešći prenosioci su izvršne datoteke, koje ima svaki OS (u Windows–u su to **.com** i **.exe**) i datoteke koje sadrže izvršni kôd (*Word* i *Excel* sadrže samoizvršavajuće makroe), za koje se ovi virusi lepe i nemaju veze sa sistemskim delom OS. Datoteke **.com** su reliktni ostaci CP/M OS i jednostavne su binarne strukture; **.exe** su savremenije, fleksibilnije i teže ih je inficirati. Nakon učitavanja prvog zaraženog programa, virusi se sele u memoriju i čekaju naredni izvršni program da ga inficiraju. Drugi metod ispoljavanja ovih virusa je izmena načina na koji računar otvara neku datoteku, umesto izmene aktuelnog programa koji aktivira datoteku. U ovom scenariju prvi se aktivira virus, a onda program. Glavna strategija nastupa ovih virusa je, da od izvršne datoteke naprave trojanca. Najpoznatiji virusi iz ove kategorije su *Jerusalem* i *Cascade*.

Višedelni virusi inficiraju i programske datoteke i *boot* sektore. Takođe, moguće je napraviti viruse koji inficiraju diskove. Neki od virusa imaju sposobnost premeštanja između *boot* sektora i programa, što ih čini težim za analizu, jer je nemoguće napraviti test datoteke bez inficiranja HD. **Programski virusi** koriste DOS-ove funkcije da bi bili rezidentni, smeštaju se na niže memorijske lokacije, dok ostali programi koriste memoriju iznad njih. Virus koji modifikuje memorijski alokacioni lanac obično sebe pomera na vrh nominalne memorije, a pokazivač vrha pomera naniže. Virusi koji inficiraju *boot* sektor obično zauzimaju vrh memorije, ali pri tom ne rezervišu taj prostor da bi se zaštitili. Oni

ne mogu biti otkriveni postupkom provere slobodne memorije, ali većina velikih programa srušiće sistem, kad se prepišu preko virusa. Određeni virus traga za slobodnom memorijom u sistemskoj zoni HD, koju koriste mnogi programi i vrlo je verovatno da će srušiti većinu sistema.

Složeni virusi su veoma opasni jer kombinuju tehnike rasprostiranja, razmnožavanja i ugrožavanja, pa su vrlo fleksibilni. Vrhunac su tehnologije programiranja virusa.

Usmereni virusi su strogo namenski programi za uništenje nekog broja određenih tipova datoteka.

Makrovirusi, preovlađujući tipovi virusa, u suštini su programi, napisani u makro jezicima, najčešći za *MS Word, Excel, Office, Access* baze i dr. Sami se zakače za dokument, a koriste makro programski jezik neke aplikacije za izvršavanje i propagaciju. Preuzimaju kontrolu nad sistemom kada se otvori ili zatvori virusom inficirana datoteka. Imaju tendenciju brzog širenja, jer korisnici često koriste aplikacije sa makro funkcijom. Prvo zahvataju standardne funkcije programa, a onda inficiraju svaku narednu datoteku koja se otvori. Mogu oštetiti i sam sadržaj datoteke. Najpoznatiji makrovirusi su *Concept*, *Marker* i *Melissa*.

Lažni virusi daju lažna upozorenja virusnog napada, sa alarmantnim upozorenjem da je računar napadnut razornim virusom i da se zahteva trenutna akcija za adekvatnu zaštitu računara. Česti su koliko i stvarni virusi. Obično izazivaju neznatne štete, ali troše operativno vreme. Neki lažni virusi mogu prevariti korisnika da izmeni konfiguraciju OS ili izbriše datoteku. Primeri ovih virusa su *Good Times* i *Bud Frogs*. Posebno su opasni u kombinaciji sa trojancem.

Šifrovani virusi sakrivaju svoj kôd ili čak inficiranu datoteku – *šifrovanjem*. Jedini tekst koji se može videti unutar inficirane datoteke je procedura dešifrovanja. Virusi su najčešće šifrovani nekom jedinstvenom procedurom, kao što je *XOR*-ovanje svakog bajta slučajno izabranim ključem, za svaku novu kopiju. Detekcija ovih virusa zasniva se na pronalaženju procedure za dešifrovanje na početku virusnog kôda.

Tipovi virusa su brojni: *virusi rezidentni u memoriji,* koji se ne gase kada se jednom pokrenu; *retro virusi,* koji zaobilaze operacije specifične za AVP; *stelt i tunel virusi,* koji izbegavaju AVP, smeštaju se u memoriji i blokiraju normalan rad i dr. [96].

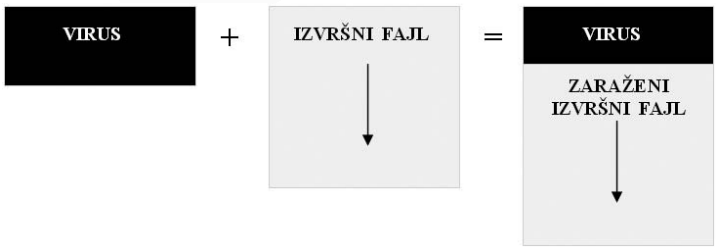
7.3.2.1. Mehanizmi širenja virusa

Savremene RM podstiču širenje virusa . Pre pojave umrežavanja računara virusi su imali mnogo manje uslova da se šire (jedino zaraženom disketom i sl.). Pojavom *intranet mreža*, virusi se mogu širiti velikom brzinom i na mnogo sofisticiranije načine. Važno je uočiti da apsolutne zaštite od novih i nepoznatih virusa nema. Najveći problem je sam OS koji je uglavnom ranjiv, bez obzira na tip. Preterana agresivnost virusa u nastojanju da se proširi, može izazvati pažnju korisnika zbog povećane aktivnosti procesora. S druge strane, ako je virus isuviše diskretan, neće uspeti da inficira veći broj datoteka.

Samoumnožavanje u postojeći izvršni kôd je ključni faktor za definisanje virusa. Kada je pokrenut, virus pokušava da se ugradi u izvršni kôd i ukoliko uspe, za taj kôd se kaže da je inficiran. Pokrenut inficirani kôd može da inficira neki drugi kôd. Širenje virusa je ograničeno na prenosne medije, u koje spadaju i izvršne datoteke, koje se prenose preko Interneta. Standardne izvršne datoteke su česta meta virusa, koji se izvršavaju sami ili ih pokreće korisnik računara. Razlikuju se dve glavne klase *mehanizma infekcije virusom – direktni i indirektni infektori.* Sa aspekta efikasnosti virusi se dele na *brze* i *spore infektore*[22].

Direktni infektori su virusi koji aktivno tragaju za datotekama, da ih zaraze. Pri tom, mogu pretraživati tekući disk, direktorijum ili selektovani direktorijum. Zatim, se učitava i izvršava inficirana datoteka. Ne ostaju u memoriji i nisu univerzalni, jer mehanizam inficiranja nije preterano efikasan. Očigledna je dodatna aktivnost procesora, posebno kada su sve datoteke zaražene. *Indirektni infektori* pri pokretanju programa inficiranog virusom, smeštaju virus u memoriju, preusmeravaju jedan ili više interaptova i potom izvršavaju originalni program. Većina ovakvih virusa inficira svaku datoteku, koja je učitana radi izvršavanja, dok neki inficiraju svaku izvršnu datoteku, koja je učitana, bez obzira na razlog učitavanja. *Brzi infektori* inficiraju datoteke koje se izvršavaju i one kojima se pristupa. Koriste i AVP da zaraze datoteke koje oni otvaraju zbog provere na virus, ali ne mogu otkriti njihovo prisustvo u memoriji. *Spori infektori* inficiraju samo datoteke, koje su u fazi kreiranja ili modifikovanja i tako zaobilaze AVP.

Infektori izvršnih datoteka najčešće koriste tehnike za *prepisivanja*, *dopisivanje ispred* i *dopisivanje iza* izvršne datoteke. Postoji metod gde se inficiraju prateće datoteke, a ne sami izvršni programi. *Tehniku prepisivanja* koriste virusi, koji prepisuju sadržaj inficirane datoteke. Korisnik, pri pokretanju ove datoteke, zapaža da nešto nije u redu sa programom, pošto se nikada ne izvršava, jer više ne postoji. Tada je već kasno da se povrati legitimni kôd. *Dopisivanje ispred izvršne* datoteke koriste virusi, koji kopiraju svoj kôd na početak inficirane datoteke. Ovo je složenija tehnika od prepisivanja i obično ne uništava program na koji se dodaje. Pri pokretanju zaražene izvršne datoteke, pokreće se maliciozni kôd, koji nakon izvršenja prebacuje kontrolu na legitimni kôd. Korisnik ne mora da primeti nikakvo čudno ponašanje programa (Sl. 7.6).

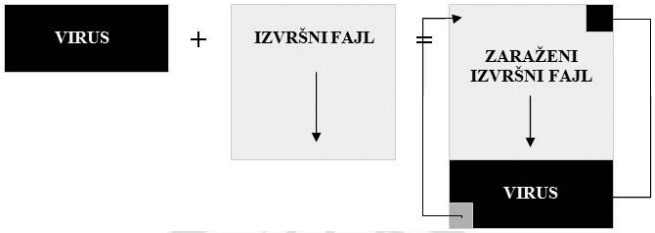


Sl. 7.7. Dopisivanje ispred izvršne datoteke

22 Mell, P., Kent, K., Nusbaum, J., *Guide to Malware Incident Prevention and Handling*, Special Publication 800-83, Novembar 2005.

Pošto ne menja sadržaj datoteke koju inficira, velika je verovatnoća da je korisnik u mogućnosti da očisti program od zlonamernog kôda.

*Tehniku dopisiv*anja iza izvršne datoteke koriste virusi, koji svoj kôd dodaju na već postojeći legitimni kôd programa. Virusi menjaju početak datoteke, koju su zarazili i naprave komandu za skok do sekcije, koja izvršava virusni kôd (Sl. 7.7).



Sl. 7.7. Dopisivanje na kraju izvršne datoteke

Nakon što se zlonamerni kôd izvrši, kontrola se vraća na legitimni program. Kao i kod tehnike dodavanja ispred programa, legitimni kôd se može povratiti uklanjanjem virusa.

Dodeljivanje virusu imena .com datoteke, tehnika za aktiviranje virusa u Windows OS, više nije dominantna na Windows OS, zbog upotrebe GUI interfejsa. Programe predstavljaju ikone i manja je verovatnoća da se pokrene pogrešan program. Međutim, mnogi korisnici i dalje kucaju u *Run* dijalogu *notepad*, *regedit* ili *.com* komande, koje i dalje prvo pokreću programe sa .com ekstenzijom.

Infektori datoteka – makro virusi koriste moćan skript jezik VBA (Visual Basic for Applications) za pisanje makroa, koji se nalazi u MS Office, WordPerfect Office, PerfectScript, ObjectPAL, AutoCAD i drugim programima. Ako se pri pokretanju ovih datoteka omogući izvršavanje makroa, šteta koju zlonamerni makroi mogu napraviti može biti ogromna.

7.3.3. Karakteristike crva

Crvi imaju nekoliko istih karakteristika kao i virusi – samo-umnožavaju se, ali kroz nešto drugačiji proces, zasebni su programi i ne zavise od izvršnog kôda. Šire se isključivo preko RM (tzv. *mrežni virusi)*. Tipičan crv se pravi modularno da lakše može promeniti funkcionalnost i sadrži *metod za upad, metod za širenje, algoritam za biranje mete, metod za pretraživanje i metod napada* (*teret)*, a svaki modul se nalazi u strukturi velikog broja crva (Sl. 7.8).



Sl. 7.8. Generička struktura crva

Kada uđe u sistem, crv mora da kopira ostatak svog kôda u sistem. U slučaju da je preuzet kao deo datoteke ili kao zaražena datoteka, metod upada i širenja su isti proces. Ako crv samo koristi neku ranjivost sistema, tada još nije u potpunosti kopiran na sistem. Najpopularniji metod za širenje crva su mehanizmi za transfer datoteka (FTP, TFTP, HTTP i drugi protokoli).

Jednom pokrenut u sistemu, crv počinje da traži nove žrtve za napad. Koristeći resurse sistema kojeg je inficirao, može da napadne e–mail adrese, umrežene računare, mrežne diskove i ostale uređaje. Mogu da skeniraju IP adrese u potrazi za žrtvama, a oni efikasniji skeniraju lokalnu mrežu i IP adrese u blizini zaraženog sistema. Ukoliko sledeća žrtva nije imuna na primenjeni metod za napad, crv se prenosi na žrtvu, izvršava svoj kôd i kopira se na sistem nove žrtve.

Teret ili metod napada predstavlja najbitniji deo kôda, koji se izvršava kada crv uspešno zarazi ciljni sistem. Ako crv ne pravi nikakvu štetu, već se samo širi sa jednog na drugi sistem, onda nema *teret*. Neki od napada koje crv može da izvrši su otvaranje zadnjih vrata (*backdoor)* za udaljenu kontrolu sistema, *zombiranje računara* ili korišćenje računarskih resursa za razbijanje šifre. Mogućnosti za napad su brojne i ograničene su samo maštom napadača.

7.3.4. Kombinovani napad

Kombinovani napad (*Blended Attack*) je slučaj malicioznog kôda koji koristi višestruke metode za širenje. Poznati *Nimda* "crv" je primer kombinovanog napada, a za širenje koristi [100]:

- *E–mail*: korisnik na ranjivom hostu otvori inficiran e–*mail* prilog, *Nimda* traži e–*mail* adrese na hostu, a zatim šalje svoje kopije na te adrese;
- *Windows zajedničke datoteke*: *Nimda* skenira hostove tražeći nezaštićenu zajedničku datoteku, zatim koristi *NetBIOS* kao prenosni mehanizam da inficira datoteke na tom hostu; kada korisnik aktivira neku inficiranu datoteku, ova će aktivirati *Nimdu* na tom hostu;
- *Web serveri*: *Nimda* skenira *web* servere, tražeći poznate ranjivosti u Windows sistemima, na koje pokušava preneti svoju kopiju i inficirati njih i datoteke;
- *Web klijenti*: Ako neki ranjivi *web* klijentski pretraživač poseti neki *web* server koji je već inficiran sa *Nimda*, radna stanica klijenta će, takođe, biti inficirana.

Tendencija korisnika je da većinu kombinovanih napada svrstavaju u crve, kao *Nimdu,* koja sa tehničkog aspekta ima karakteristike virusa, crva i mobilnog kôda.

7.3.5. Trojanci i ostali maliciozni programi

Trojanski konj (trojanac) se predstavlja i ponaša kao benigni program, koji u pozadini izvršava maliciozne aktivnosti. Sastoji se od *serverske* komponente, koja se ubacuje u računar korisnika i *klijentske* komponente, kojom upravlja napadač. Klasičan primer ubacivanja trojanca je program, koji postavlja *login* upitnik i očekuje da korisnik unese ime i lozinku. Kada korisnik unese ove podatke, program ih šalje napadaču, a korisniku izbacuje grešku pri prijavljivanju na sistem.

Napadači su razvili brojne tehnika da prikriju prisustvo trojanaca. Neke su jednostavne, ali dosta uspešne kod nedovoljno stručnih korisnika, kao npr. promena imena izvršnih datoteka. Većina korisnika Windows OS zna da ne treba pokretati izvršavanje sumnjivih .**exe** datoteka. Napadači, skoro bez izuzetka, pokušavaju da kamufliraju **.exe** datoteke. Jednostavan način za ovo je davanje imena izvršnoj datoteci sa, npr. **.txt** ekstenzijom. Korisnik, koji je podesio sistem da ne prikazuje ekstenzije, videće samo **.txt** ekstenziju. Nešto složeniji način je stavljanje velikog broja praznih mesta u ime datoteke, tako da i korisnik, koji ima uključeno prikazivanje ekstenzija, može prevideti pravu ekstenziju.

Za razliku od Windows OS, UNIX i na njemu bazirani sistemi, ne pridaju veliki značaj ekstenzijama datoteka. Mnogi tipovi datoteka za Windows platforme se mogu upotrebiti za skladištenje i pokretanje izvršnog i skript kôda. Pored najpoznatije **.exe** ekstenzije, trojanac koristi i **.api, .bat, .wma, .chm, .com, .cpl, .dll, .sys, .scr** i druge ekstenzije[23].

Trojanci koriste i tehnike oponašanja legitimnih imena procesa. Na Windows platformi, skoro u svakom trenutku, u listi aktivnih procesa *Task Manager*–a mogu se videti nazivi kao *iexplorer.exe, explorer.exe, smss.exe, svchost.exe, system, services.exe* i drugi. Trojanci se često kriju između ovih procese, čak i sa unikatnim imenima kao *win.exe, antivirus.exe* i slično, koje administrator očekuje da vidi u sistemu. Štaviše, ako napadač svog trojanca nazove imenom procesa koji je vitalan za rad *Windows*–a, Windows neće dozvoliti da ga administrator ugasi. Druge tehnike su dosta složenije i mogu se oslanjati, npr. na izmenu izvornog kôda legitimnih programa već instaliranih na sistemu. Jedna od često korišćenih tehnika je udruživanje dva, ili više procesa, od kojih je jedan trojanac, a ostali benigni legitimni programi. Za ovo se koristiti neki *wrapper* program – *EliteWrap*, *Saran Wrap*, *TOPV4*, *Trojan Man* itd. Pokretanjem ovog programa dolazi do razdvajanja na više zasebnih procesa, koji mogu da se vide u *Task Manager*–u.

23 www.sophos.com/blogs/gc/g/2008/08/08/up-to-1800-profiles-hit-by-malware-attack-says-facebook/, (Posećeno: 2.12.2009.)

Zadnja vrata (*backdoor*, *trapdoor*) predstavlja svaki mehanizam, koji zaobilazi normalnu kontrolu pristupa u sistemu, pri čemu može da ostvari dovoljno privilegovan pristup sistemu. Programeri često namerno stvaraju zadnja vrata u kôdu, radi legitimnih razloga (npr. da bi izbegli ostavljanje tragova u logovima pri testiranju i razvoju programa). U samostalne *backdoor* programe spadaju i svi RAT (*Remote Administration Tool*) programi, koji koriste brojne službe tehničke podrške proizvođača programa i administratori za udaljeni pristup i rad na korisnikovom računaru. *Backdoor* i trojanac mogu se slično ponašati, ali postoje bitne razlike. *Backdoor* je program koji samo omogućava zaobilazni pristup računaru, dok trojanac omogućava to isto, ali varajući korisnika da je neki korisni program. *Backdoor* napadaču može da obezbedi sledeće vrste pristupa:

1. *eskalaciju lokalne privilegije*, promena svoje privilegije u administratorske,
2. *udaljeno izvršavanje komandi* na napadnutom računaru,
3. *udaljeni pristup komandnoj liniji* i izvršavanje svih radnje na sistemu i
4. *udaljena kontrola GUI* napadnutog sistema i kontrola miša i tastaturu.

Svi ovi metodi se zasnivaju na kontroli napadnutog računara, uglavnom sa udaljene lokacije. Načini instaliranja *backdoor* na neki sistem su različiti. Napadač može iskoristiti neku uobičajenu grešku u sistemu ili ranjivost konfiguracije, ući u sistem i potom sam instalirati *backdoor* za sledeći ulazak, pomoću virusa, crva ili malicioznog skript kôda koji se izvršava u pretraživaču.

Špijunski program (*Spyware*) je program koji sakuplja informacije sa računara korisnika (npr. korisnička imena i lozinke, e-*mail* adrese, bankovni računi, licence, itd.) i prosleđuje ih napadaču. Pri definisanju tipa malicioznog programa odlučuju detalji. Ako se od korisnika na pasivan način saznaje korisničko ime i lozinka, u pitanju je *spyware*, a ako je uključena obmana korisnika – u pitanju je trojanac.

Logičke bombe su slične trojancu po metodi napada. Uglavnom se sastoje od dva dela – *tereta*, koji izvršava neki maliciozni kôd i *okidača* – dela kôda koji pokreće izvršavanje malicioznog tereta. Okidač se može aktivirati i u slučaju odsustva nekog događaja. Logičke bombe mogu da zavise od izvršavanja nekog drugog programa, a mogu biti i napravljene kao samostalne aplikacije, od čega zavisi da li su parazitske ili ne.

Maliciozni skriptovi (mobilni kôdovi) dovode do prenosa ili izvršavanja malicioznog kôda. Tipičan predstavnik je *Cross Site Scripting* napad na web aplikacije. To je aktivni program koji se prenosi sa udaljenog sistema na lokalni, a zatim izvršava na lokalnom sistemu bez eksplicitne instrukcije korisnika. Često služi kao mehanizam za prenos virusa i crva ili trojanaca do radne stanice korisnika. U drugim slučajevima, koristi ranjivosti sistema da izvrši svoje akcije, kao što su neovlašćen pristup podacima ili kompromitacija ruta. Popularni prenosioci mobilnih kôdova su *Java applets, ActiveX, JavaScript* i *VB-Script*.

7.3.6. Metodi skrivanja malicioznih programa

Autori malicioznih programa koriste brojne *antiforenzičke aktvinosti*[24] da se zaštite od AVP, korisnika i administratora, kao što su *samozaštita* od detekcije na bazi potpisa, forenzičke analize kôda i detekcije malicioznog kôda u sistemu i *ometanje* funkcionalnosti AVP, barijera, IDPS i drugih programa za zaštitu.

Polimorfizam je proces kroz koji maliciozni program modifikuje svoj kôd, da bi izbegao detekciju, pri čemu ne menja funkcionalnost. Ovim se virusni kôd može dinamički menjati, svaki put kada je virus pokrenut. U tom slučaju AVP, naučen da prepoznaje samo ranije otkrivene potpise malicioznog kôda – neće ga otkriti. Najjednostavnija tehnika polimorfizma sastoji se u slučajnoj izmeni imena promenljivih i imena funkcija, pre inficiranja novih datoteka. Drugi metod se sastoji u dodavanju dela kôda koji nema značajnu ulogu, npr. dodavanje broja i kasnije oduzimanje iste vrednosti od neke promenljive. Naprednija tehnika je izmena redosleda, kojim se izvršavaju instrukcije u kôdu. U isto vreme, potrebno je zadržati nepromenjenu funkcionalnost programa. Polimorfizam se sve ređe viđa kod modernih malicioznih programa, pošto, npr. trojanci uglavnom nemaju sposobnost širenja, pa nije ni potrebno da menjaju svoj kôd.

Metamorfoza je konstantno menjanje funkcionalnosti virusa pri njegovom širenju, obično na jednostavne načine, a da bi se izbegla detekcija. Od 1992. godine mnoge AV kompanije su ugašene, jer nisu uspele da razviju efektivne odbrambene mehanizme protiv polimorfnog i metamorfnog kôda, koji je u to vreme počeo masovno da se koristi. Posebna polimorfnu tehnika je šifrovanje kôda.

Šifrovanje kôda virusa primarno služi za onemogućavanje ispitivanja kôda. Šifruje se čitav kôd, osim dela instrukcije za dešifrovanje kod izvršavanja. Obično se koristi slučajno izabrani ključ za šifrovanje, koji se zapiše u kôdu. Prvi alat za jednostavno dodavanje polimorfnog šifrovanja je MtE (*Mutation Engine,* 1992).

Maskiranje je tehnika koja se upotrebljava uglavnom za sprečavanje analize. Kako se sve više detekcija malicioznog kôda zasniva na ponašanju programa, a ne kôdu, tehnika polimorfizma i ostale više nisu od ključnog značaja autorima virusa.

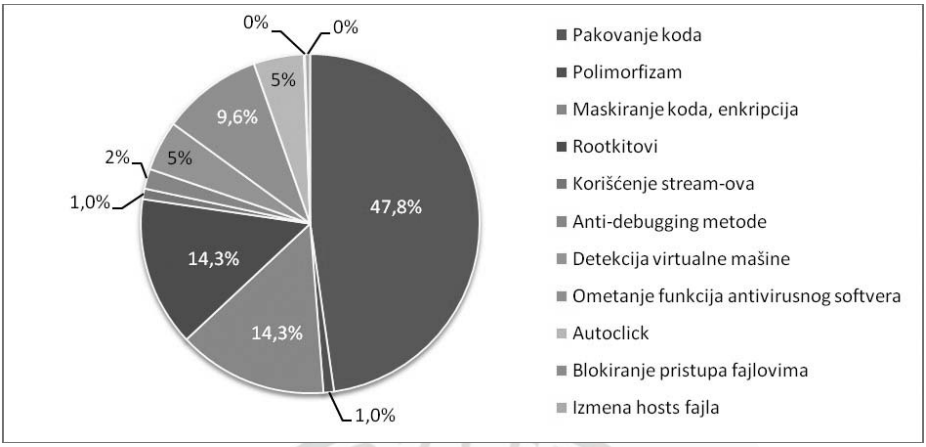
Tehnike sakrivanja se odnose na prikrivanje prisustva malicioznog programa na računarskom sistemu. Primitivan metod, koji se često koristi kod jednostavnih virusa, sastoji se u postavljanju atributa *hidden*. Na ovaj način, datoteka se neće prikazati u direktorijumu, ako je sistem podešen da ne prikazuje sakrivene datoteke. Napredniji metod se sastoji u presretanju zahteva AVP za sadržajem datoteke i prezentovanje čiste verzije datoteke AVP skeneru.

Rutkit tehnike **(***Rootkits***)** se sve više uspešno koriste za sakrivanje aktivnosti trojanaca, jer većina korisnika Windows OS koristi administratorske naloge. Otkriveni su tokom 2004. godine u istraživačkoj laboratoriji kompanije *Kasperski.* Prvi rutkit se nije mogao videti u Windows listi aktivnih procesa i datoteka i predstavljao je revoluciju

24 Namenjene za skrivanje tragova i zaštitu od otkrivanja tehnikama i alatima digitalne forenzike.

u industriji virusa [110]. Sam termin *rootkit* potiče od Unix alata, koji su omogućavali korisniku pristup administratorskim (*root*) komandama, bez posledica i znanja administratora sistema. Danas, termin *rootkit* pokriva grupu alata i tehnika koje se koriste za sakrivanje ubacivanja i prisustva trojanaca, virusa i crva u sistemu. Ovde se podrazumeva i sakrivanje na listi aktivnih procesa, u ključevima registara kao i u skenerima mrežnog saobraćaja. Snaga rutkitova leži zapravo u slabosti AVP, koji uglavnom ima privilegije kao i svi drugi programi na sistemu. Ako korisnik nema pristup nekim resursima sistema, nema ni AVP. Princip sakrivanja pomoću rutkita je isti kao i kod primitivnih DOS *stelt* virusa. *Kompresija* je najzastupljeniji i možda najstariji savremeni metod samozaštite pakovanja kôda, jer je, u prvim godinama razvoja malicioznog programa kada se veličina HD merila u megabajtima, veličina datoteke bila jako bitna. Kompresovan kôd je teže pregledati i istražiti da li je maliciozan. Takođe, mnoge varijante crva i virusa se razlikuju u samo nekoliko linija kôda, ali nakon kompresije, potpuna struktura datoteke se menja i AVP–u je teže da otkrije modifikacije. Mnogi rutkitovi modifikuju lanac sistemskih poziva (*Execution Path Modification*). Kada se naiđe na proces, koji nosi informaciju o nekom aktivnom procesu, rutkit ga presreće i modifikuje. Uobičajena rutkit tehnika je i DKOM (*Direct Kernel Object Modification*), koja se najbolje opisuje kao *insajder* koji menja informacije ili komande još na njihovom izvoru. Ovi rutkitovi menjaju sistemske podatke. Moguće je sakriti i čitave datoteke u alternativnim tokovima podataka – ADS (*Alternate Data Streams*). ADS predstavljaju malo poznatu osobinu NTFS *sistema datoteka*. Datoteke sa ADS je jako teško otkriti, jer dodatne informacije zapisane u ADS–u operativni sistem ne uračunava u veličinu datoteke. Štaviše, kada se pokrene, npr. program koji nosi nekog trojanca u ADS, njegovo prisustvo se neće manifestovati u Windows *Task Manager*–u [114].

Deaktivacija AVP, koji je aktivan na zaraženom sistemu, još je jedan način za skrivanje malicioznog kôda. Istog trenutka kada se sistem zarazi, maliciozni kôd pokušava da ugasi procese koji pripadaju AVP programu. Na ovaj način, AVP neće ažurirati najnovije potpise virusa. Dobar primer predstavlja *ProcKill* trojanac, koji sadrži listu od preko 200 procesa koji pripadaju AVP i programima barijera. Kada zarazi sistem, *ProcKill* redom čita svoju listu i ukoliko nađe pokrenut proces sa liste, pokušava da ga ugasi [112]. Složeniji metod, kojeg koriste mnogi savremeni crvi, sastoji se od blokiranja svake komunikacije između sistema i servera poznatih AV kompanija. Kako se AVP i dalje vidi u listi procesa u sistemskoj listi poslova (*system tray*), korisnik i ne sumnja da je zaražen. Ovu tehniku je prvi koristio *MTX* virus/crv, 2000. [111]. Na Sl. 7.9 zbirno su prikazane najčešće tehnike samozaštite koju koriste maliciozni programi.



Sl. 7.9. Najčešće korišćene tehnike samozaštite malicioznih programa [111]

7.4. DISTRIBUCIJA MALICIOZNIH PROGRAMA

Veoma mali procenat malicioznih programa se ne prenosi putem Interneta. Takođe, maliciozni program retko ima za cilj da zarazi samo jedan računar, pa je prenos putem Interneta najbrži način da se inficira što veći broj računara. Ako je cilj kompromitacija sistema zaštite, napad ne mora doći sa Interneta – maliciozni program može da se instalira putem USB–a ili *Bluetooth* veze sa mobilnim telefonom. Usmereni napad na jedan računar je i najopasniji, zbog mogućnosti korišćenja naprednih metoda napada poput socijalnog inženjeringa i drugih alata. U dužem periodu, ne postoji sistem čija se bezbednost ne može ugroziti.

Iskoristive ranjivosti RS omogućavaju napadaču da naruši integritet sistema. Maliciozni program koji iskoristi ranjivost naziva se *exploits*. Ranjivosti čine, na primer*, slaba lozinka, nedovoljna provera upita, slaba konfiguracija, greška u softveru ili hardveru* itd., a vrlo se često koriste kao sredstvo za distribuciju malicioznog programa. Na primer, automatskim preuzimanjem sa Interneta, korisnik može da preuzme zaraženu datoteku ili aktivira *buffer overflow* ranjivost. Američka nacionalna agencija za bezbednost (NSA) je sastavila listu (12.01.2009) od 25 uobičajenih programerskih grešaka, koje mogu dovesti do iskoristive ranjivosti [113]. Samo dve od ovih ranjivosti su tokom 2008. godine ugrozile bezbednost 1.5 milion Internet lokacija i *zombirale* računare posetilaca ovih lokacija. Na vrhu liste ranjivosti nalaze se nepotpuna validacija podataka unetih od strane korisnika, nemogućnost da se održi struktura baze podataka i *web* sajta i druge. Sve ove greške mogu da dovedu do širenja ili izvršavanja malicioznog kôda.

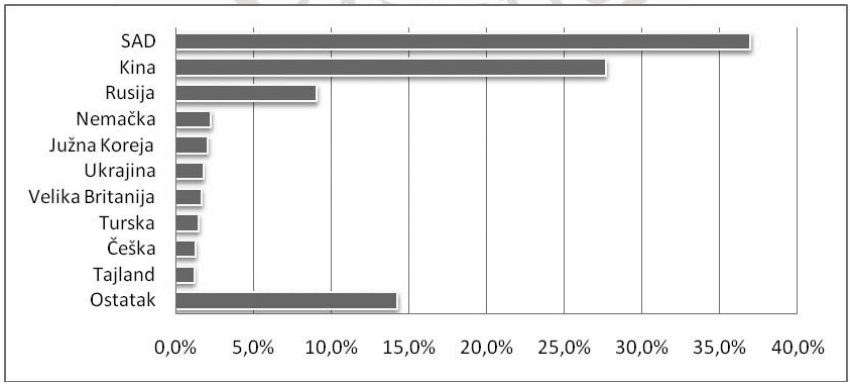
Cross Site Scripting (XSS) je tip ranjivosti, koja se obično nalazi u *web* aplikacijama koje greškom dozvoljavaju ubacivanje malicioznog kôda u *web* stranice koje mogu da vide drugi korisnici. U 2007. godini, XSS je činio oko 80% svih dokumentovanih bezbednosnih propusta [115]. XSS kôdovi su napisani u skript jezicima – *JavaScript, ActiveX, ActionScript, RSS i* drugim, a izvršavaju se na klijentskom pretraživaču.

SQL Injection je tehnika za ubacivanje kôda koja iskorišćava ranjivosti u sloju baze podataka neke aplikacije. Do iskorišćavanja ranjivosti dolazi, kada napadač ubaci znakove u npr. legitimno polje za korisničko ime, što dovodi do nepredviđenog izvršavanja upita nad bazom.

Automatsko preuzimanje (Drive By Download) predstavlja ozbiljnu ranjivost i metod širenja malicioznog programa. Pod terminom se podrazumeva svako preuzimanje programa koje korisnik nije odobrio ili je prevaren da ga odobri. Ova se ranjivost iskorišćava posetom zaraženom *web* sajtu, otvaranjem e–mail poruke ili klikom na zamaskirani link, obično u *web* pretraživačima, e–mail klijentima ili OS.

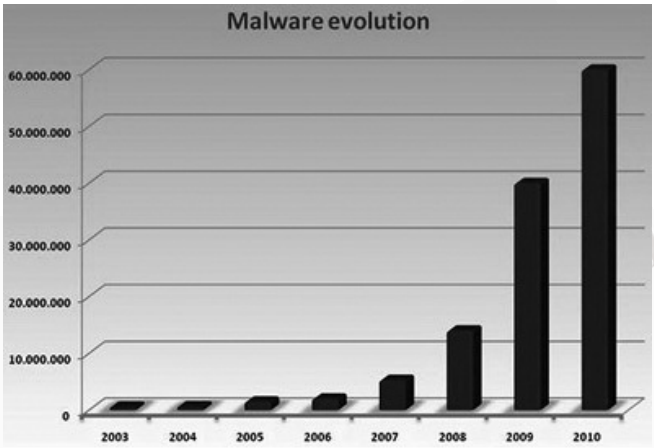
Phishing (pecanje) je proces u kome napadač pokušava da pribavi osetljive informacije od žrtve (broj bankovnog računa, PIN kôd itd.), obmanjujući je lažnom e–*mail* porukom, lažnom *web* lokacijom ili lažnim *popup* prozorom, koji izgledaju kao legitimni. Iako po definiciji ne spada u maliciozni program, korisnik vrlo često bude žrtva *phishinga* zahvaljujući malicioznom dejstvu virusa ili crva koje unose.

Zahvaljujući propustima u Internet pretraživačima i neznanju korisnika, jedan od dominantnih načina za distribuciju malicioznih programa su zaražene *web* stranice. Procena je da je od 100% *web* lokacija koje prenose maliciozne programe, samo 15% za tu svrhu i napravljeno. Ostalih 85% je napadnuto i zaraženo bez znanja administratora, uglavnom *SQL injection napadom* (Sl. 7.10).



Sl. 7.10. Države koje hostuju najviše zlonamernih program [116]

U prvih 10 meseci 2010. generisana je 1/3 (34%) svih do sada malicioznih programa (*malvera*) na Internetu - oko 20 miliona novih (uključujući i modifikovane stare). To su automatski otkrile baze podataka kompanija širom sveta, koje analiziraju i klasifikuju 99,4% od svih detektovanih pretnji. U 134 miliona posebnih fajlova nalazi se 60 miliona *malvera* (virusa, crva, trojanaca i dr.). Prosečno je dnevno generisano na Internet 63.000 (53.000 u 2009.). Od toga je 54% *malvera* aktivno samo 24 časa, što otežava detekciju. Ipak, godišnji porast je u opadanju u odnosu na 2003. – 100% u odnosu na 2002., a u 2010 je rast za 50% u odnosu na 2009. (Sl. 7.11).[25]



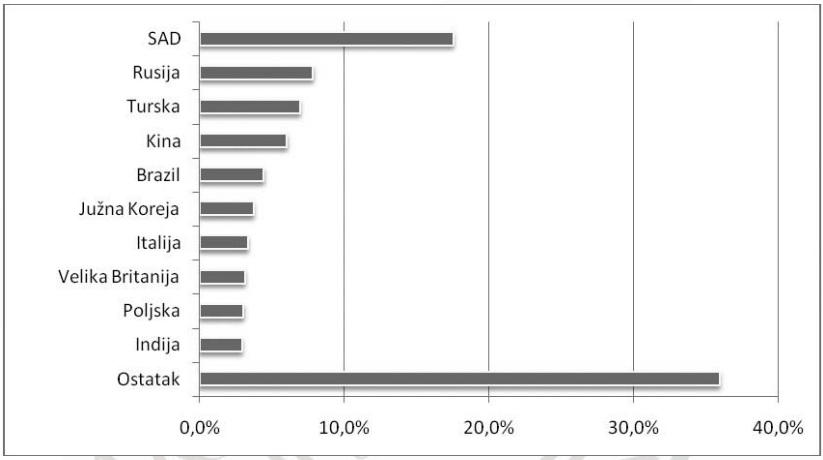
Sl.7.11. Razvoj malicioznih programa (malvera) u periodu 2003-2010.

***Spam* i zaražene e-*mail* datoteke** su najzastupljeniji metod distribucije malicioznih programa. Kompanija *Sophos* tvrdi da *spam* čini 97% svih poslovnih pisama – prodaja ilegalni proizvoda, slanje e-*mail* poruka za preuzimanje i instaliranje nekog malicioznog programa itd. Tokom 2008., svaki 714–ti e-*mail* je nosio zaraženu datoteku, u odnosu na 2005. godinu kada je svaki 44–ti bio zaražen. Za ovaj pad je najviše zaslužna medijska hajka na viruse poput *I Love You* i *Melissa*. Prosečan korisnik ređe otvara sumnjive datoteke, a napadači su pronašli nove načine za napad. Ipak, moguće je da će e-*mail* ponovo postati značajnije sredstvo za širenja malicioznih programa, pošto u savremenom e-poslovanju šifrovan *e-mail* postaje značajna alternativa bezbednijem PKI sistemu. Nove ranjivosti u Word **.doc**, ili Adobe **.pdf** datotekama, na računarima koji nemaju instalirane najnovije bezbednosne popravke, mogu izazvati veliku štetu. *Spam* se uglavnom širi pomoću umreženih računara čiji korisnici nisu svesni da su im računari *korumpirani*. Ove mreže se nazivaju *botnet* – mreže robotizovanih računara. *Bot* računar sadrži program koji omogućava da se sa tim računarom daljinski upravlja, često sa centralnog servera, koji šalje komande, a *bot* ih izvršava bez znanja korisnika.

25 *Luis Corrons, Technical director of PandaLabs,* 24.11.2010.

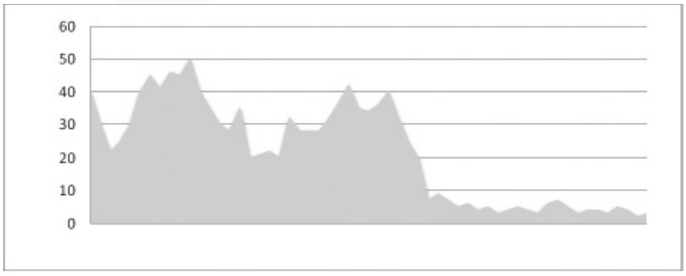
Takav program koji omogućava udaljenu administraciju ne mora da bude zlonameran. Windows XP dolazi sa fabrički omogućenom podrškom za udaljenu administraciju, koju treba onemogućiti. *Botovi* ne moraju uvek biti aktivni; ako samo osluškuju instrukcije sa servera, nazivaju se – *zombi* računari.

U praksi jedan napadački server uvek kontroliše veći broj *bot* umreženih računara. Najrasprostranjeniji način na koji *botovi* komuniciraju sa serverom je preko IRC-a (*Internet Relay Chat)* servisa. *Bot* mreže se mogu iskoristiti za prikupljanje e-*mail* adresa *kilogeima* za slanje *spama*, hostovanje malicioznog programa, *phishing web* sajtove, razbijanje šifri, DoS/DDoS napade i dr. Brojne države šire *spam* poruke, a najviše spama potiče iz SAD – 17,5% (Sl. 7.11).



Sl.7.12. Države iz kojih se šalje najviše spam poruka [116]

Poznat je slučaj jedne ruske hosting kompanije *McColo,* koja je na svojim serverima hostovala komandne centre za pet velikih *botnet* mreža – *Srizbi* (Zlob), *Mega–D, Rustock, Dedler i Storm*. Kada su *McColo* i *botnet* mreže isključeni sa Interneta (11. 10. 2008. u 13:23), došlo je do pada *spam* poruka za čak 75% (Sl. 7.12).



Sl. 7.13. Pad količine SPAM poruka tokom 11.10.2008. [116]

Napad zastrašivanjem *(Scareware)* je eskalirao 2008. godine, oslanjajući se na taktiku zastrašivanja i navođenja potencijalne žrtve da instalira lažni AVP. Žrtve se mame lažnim alarmom o ugroženoj bezbednosti njihovog računara putem *popup* prozora na zaraženim sajtovima ili putem *spam* poruka. Na primer, južnokorejska AVP kompanija *Lee Shin* je od 2005. godine zaradila preko 9,8 miliona dolara nudeći besplatni *anti-spyware* program, koji je prikazivao lažna upozorenja o ugroženosti sistema i navodio korisnike da kupe naprednu verziju programa njene kompanije [102].

Socijalni inženjering je drastičan primer napada na *Facebook* naloge, koje poseduje i aktivno koristi više od 200 miliona osoba i organizacija [104]. Samo u avgustu 2008. godine, *Facebook* je objavio da je preko 1800 korisnika napadnuto trojancem i njihovi nalozi korišćeni za slanje *spama* i malicioznih programa. *Facebook* je moćan alat u rukama napadača, jer niko ne očekuje da je poruka koju je upravo dobio od najboljeg prijatelja zapravo zaraženi program. Hiljade korisnika je bilo prevareno, kada su od prijatelja dobili poruku da je on tokom puta u Nigeriji bio opljačkan i moli vas da mu pošaljete novac preko *Western Uniona* i sl. [109].

P2P (*Peer–to–peer*) mreže, specijalizovane za distribuciju datoteka između korisnika, uglavnom se koriste za distribuciju ilegalnih datoteka i piratizovanog softvera. Neretko su ove datoteke inficirane malicioznim programom, a korisnici ovih mreža se oslanjaju na preporuke drugih korisnika u vezi sa tim da li je program inficiran ili ne.

USB uređaji i pojava *U3 smart* diska doneli su i nove tehnike za napad. *USB Switchblade* sadrži U3 USB memoriju koja je u stanju da instalira zadnja vrata i preuzme osetljive informacije sa sistema na koji je povezan. Za razliku od tradicionalnih USB 2.0 uređaja, U3 memorije se same pokreću kada se uključe u sistem. Nakon uključivanja u Windows OS, *USB Switchblade* u pozadini sakuplja informacije kao što su heševi lozinki, IP adrese, istorije i *auto–fill* informacije iz Internet pretraživača, AOL *Instant Messenger* i MSN Messenger lozinke i instalira zadnja vrata na sistemu. Ovaj alat koristi osobinu U3 drajva da napravi virtuelni CD–ROM na USB memoriji i na taj način omogućava Windows *auto–run* funkciju. U 2008. godini zabeležen je interesantan slučaj distribucije malicioznog kôda na međunarodnoj svemirskoj stanici ISS, kada je jedan astronaut slučajno koristio USB memoriju koja je nosila crva *W32.Gammima.AG* [105].

Optički mediji i hardver sa originalnim programom koji kompanije distribuiraju (npr. CD i DVD), takođe, prenose i maliciozne programe. Mnoge svetski poznate kompanije su imale negativan publicitet na ovaj način, a korisnici su bili primorani da *čiste* kompjutere od virusa i crva koje su dobili od proizvođača. *Samsung* je distribuirao crva *W32.Sality. AE* zajedno sa programom za digitalni ram za slike, a *Asus* je u oktobru 2008. Godine, u Japanu pustio u prodaju *Eee Box mini PC* zaražen crvom *W32/Usbalex* [113].

Mobilni telefoni i Wi–Fi uređaji, takođe, su ranjivi i korisnici mogu da očekuju sve veći broj napada. U 2008. godini pojavili su se *Apple 3G iPhone* i *T–Mobile G1* – prvi telefon koji koristi ranjivi *Google Android* OS. Jedna od posledica napada je, npr. nemogućnost da se prikaže čitava URL adresa u Internet pretraživaču, usled malih dimenzija ekrana, pa korisnici ne mogu da razlikuju lažne *phishing* stranice od legitimnih. Kako savremeni

mobilni telefoni imaju sve veći značaj u mobilnom poslovanju, poznavanje malicioznih programa namenjenih mobilnim telefonima ne treba zanemariti. *Smart telefoni* imaju sve opcije računara i već postoji veliki broj malicioznih programa namenjenih za napade na ove telefone [106].

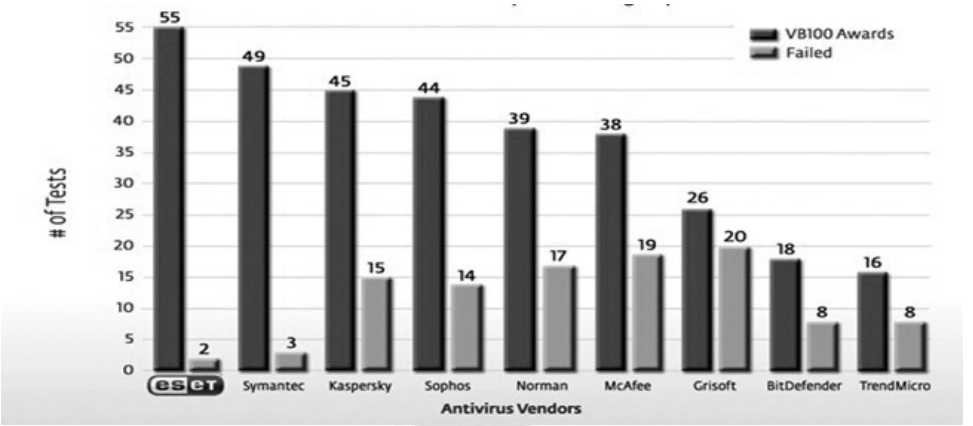
7.5. MERE ZAŠTITE I OPORAVAK SISTEMA OD MALICIOZNIH NAPADA

Za odbranu RS/RM od dinamički promenljivih pretnji i malicioznih napada, optimalno je primeniti različite U, O i T kontrole u *bezbednoj arhitekturi sistema sveobuhvatne, višeslojne zaštite*, kao što su [50, 83]: *obuka i razvoj svesti o potrebi zaštite*; *fizička i personalna* zaštita; *višeslojna antivirusna zaštita*; *nadzor i kontrola log tragova*; *logička AC i politika privilegija*; *blokiranje aktivnog sadržaja*; *izolacija mrežnom barijerom*; *primena kriptoloških mehanizama i tehnologije digitalnog potpisa*; *procedura jake autentifikacije korišćenjem digitalnih sertifikata*; *korišćenje jakih ključeva i česta izmena*; *zaštita IP adresa servera* i *korišćenje smart kartica* za generisanje digitalnog potpisa i bezbedno čuvanje ključeva i drugih kriptografskih parametara.

Procedura za oporavak sistema od malicioznih napada i mere zaštite moraju biti deo strategije za održavanje stanja bezbednosti informacija na prihvatljivom nivou rizika. Glavni zahtevi su osposobiti sistem kroz procedure za *izolaciju inficiranih sistema, uklanjanje malicioznog programa iz sistema, restauraciju integriteta sistema nakon napada (obično iz rezervne kopije) i oporavak servisa sistema*. Procedure za oporavak sistema moraju biti jasno dokumentovane, regularno testirane i treba da sadrže proces za akcije korisnika i obavezno izveštavanje u slučaju virusne infekcije. U antivirusnu borbu treba uključiti poverljive provajdere zaštite (snabdevače AVP), kao i glavne ISP koji mogu potpuno ukloniti botnet i maliciozne napada sa Interneta[26], zbog akumuliranja znanja o vrsti napada, odbrani i proceni štete i resursa za oporavak sistema. U literaturi [32] dati su kriterijumi za izbor AVP, elementi za izradu procedura za oporavak i standardni stepeni kontrole intenziteta malicioznih programa. U razvoju sistema zaštite i odbrane od malicioznih napada na sisteme u mrežnom okruženju, glavni je problem identifikovanje različitih tipova zloupotreba mrežne infrastrukture, da bi se projektovale adekvatne mere zaštite. Tehnička rešenja uključuju programska (AVP) i hardverska. Grafikon na slici 7.13. prikazuje najefektivniji antivirusni program u 2009. godini i njegov nivo zaštite od malicioznih programa. Primer hardverskog rešenja je *F–Secure Messaging Securiti Gatevay, X* serije koji obezbeđuje potpunu zaštitu od neželjene pošte, virusa i drugih malicioznih programa. *F–Secure* uređaji kombinuji MTA[27], anti–spam, antivirusni i modul za filtriranje sadržaja e–pošte. Veoma je jednostavan za instalaciju, ima visoke performanse, a dizajniran je da zaštiti male i srednje organizacije.

26 www.searchsecurity.com, Robert Westervelt, News Editor, (Posećeno 17 Marta 2010).

27 Engl.: MTA (*Mail Transfer Agent*) – agent za prenos elektronske pošte.



Sl. 7.14. Pregled efektivnosti antivirusnih programa u 2009. godini [32]

7.6. REZIME

Sa razvojem RM i umrežavanja, rastu i potencijalne pretnje od različitih napada spolja i iz mreža intranet tipa. Moguće su brojne *taksonomije* pretnji u odnosu na različite kriterijume, a *krajnji cilj svake je, da se specijalistima zaštite i korisnicima obezbedi lakše definisanje i identifikovanje različitih tipova pretnji za* IKTS*.* Prema *prirodi izvora* pretnje se dele na *slučajne* i *namerne*. Kako iza svih malicioznih napada stoje ljudi, profilisanje kompjuterskih kriminalaca je značajna aktivnost u borbi protiv kompjuterskog kriminala. Ključni tipovi napada su *destrukcija, izmena podataka, prekid servisa (DoS/DDoS napadi), špijunaža i neovlašćeno korišćenje*.

Za zloupotrebu/kompjuterski kriminal potrebni su *motiv, sredstvo i prilika*. *Opšti motivi* hakera su znatiželja, novac, moć, osveta i dr., a *posebni* – intelektualni izazov, radoznalost, borba za prestiž i dr. *Sredstva* su nivo veštine i tehnološki kapaciteti sa kojima hakeri izvršavaju kriminal, a *prilika* – iskoristiva ranjivost, koja se često teško određuje zbog antiforenzičkih aktivnosti za skrivanje tragova napada. *Maliciozni program* je kôd koji se tajno ubacuje u drugi program sa namerom da se unište podaci, pokrenu destruktivni programi ili kompromituje bezbednost i naruši CIA informacija. Generalno, dele se na *viruse, crve, trojance, mobilni kôdove, kombinovane napade i dr*.

Računarski virus je program koji *inficira* ostale programe, modifikujući ih tako da uključuju njegovu naprednu kopiju. Virus se može širiti kroz računarski sistem i mrežu, koristeći autorizaciju svakog korisnika. Inficiran program se, takođe, ponaša kao virus pa se infekcija širi. *Crvi* su maliciozni programi koji menjaju ili uništavaju podatke i šire svoje kopije ili delove na druge računare, obično preko mreža, pa ih nazivaju i *mrežni virusi*. *Mobilni kôd* je aktivni program koji se prenosi sa udaljenog sistema na lokalni, a zatim izvršava na lokalnom sistemu bez eksplicitne instrukcije korisnika; često služi kao me-

hanizam za prenos virusa, crva ili trojanaca do računara korisnika. *Kombinovani napad* je slučaj malicioznog kôda, koji za širenje koristi višestruke metode: *e–poštu*, *zajedničke datoteke Windows*, *web servere*, *web klijente* ili u *peer–to–peer* arhitekturi sistema. Sa tehničkog aspekta, kombinovan napad ima karakteristike virusa, crva i mobilnog kôda. *Trojanac* je prosta forma zlonamernog programa, naizgled interesantna korisnicima; prikazuje poruke, briše datoteke ili diskove, ali ne inficira ostale izvršne datoteke, jer se ne replicira, pa zato i nije u kategoriji virusa.

Mere zaštite od malicioznih kodova treba da uključuju *sveobuhvatnu*, *višeslojnu* zaštitu IKTS – obuku i razvoj svesti o potrebi zaštite, fizičku i personalnu zaštitu, AVP, skener integriteta RM/RS, nadzor i reviziju kontrolnih informacija itd.

7.7. KLJUČNI TERMINI

***Boot* virusi:** inficiraju sistem kada korisnik pokuša da butuje sa inficiranog medija.

Crv: kompletan program koji se umnožava bez *inficiranja* ostalih programa.

Haker*:* znatiželjni mladi poznavalac računara, koji neovlašćeno upada u tuđe računare, uglavnom bez malicioznih namera, a u želji za sticanjem novih znanja.

Kompjuterski kriminalci*:* rade sa/bez računara, kradu tuđe tajne i novac, uništavaju datoteke, OS ili menjaju podatke Web stranica ili baza podataka.

Logička bomba*:* kôd ubačen u legitiman program, dizajniran da se aktivira u tempirano vreme i proizvede rezultate koje legitimni korisnici programa ne žele.

Maliciozni kôd: program koji se tajno ubacuje u drugi program sa namerom da se unište/izmene podaci ili na drugi način kompromituje bezbednost računara.

Mobilni kôd: nalazi se u aktivnom sadržaju (*JavaScript, Java Applets i ActiveX*) web dokumenta namenjenom za prezentaciju; skriva se u pretraživaču klijenta.

Trojanac: program, atraktivan legitimnom korisniku (igrica, alat), koji skriva malignu nameru (npr. krađa pasvorda); ubacuje se u sistem na brojne načine.

Virus: kôd ubačen u legitiman program, napisan da se sam reprodukuje kopiranjem u druge legitimne programe.

Zamka (*trapdor*): metod dobijanja kasnijeg pristupa nekim delovima IKTS izvan normalne procedure; često ih ostavljaju programeri kao bag, koji otkrivaju hakeri.

7.8. PITANJA ZA PONAVLJANJE

1. Krajnji cilj svake taksonomije pretnji je da se:
   a. obezbedi lakše definisanje i identifikovanje različitih tipova pretnji
   b. ukaže na različitu prirodu izvora, intenziteta i verovatnoće uticaja pretnji
   c. omogući korisnicima lakše otkrivanje napadača
2. Koje su od navedenih pretnji istovremeno veštački izazvane i vanredni događaj?:
   a. nepotpune rezervne (bekapovane) kopije
   b. nestanci električnog napajanja
   c. poplava u zgradi i računarskom centru zbog pucanja vodovodnih cevi
   d. serveri zaraženi virusom
   e. izbio požar u zgradi

3. U IKTS sa pristupom Internetu velike brzine, zaposleni imaju instalirane modeme, ako veza velike brzine ne radi, mogu birati web pretraživače i ažurirati svoje računare. Koja mera zaštite je najbolja za odbranu od potencijalnih pretnji?:
   a. povećati broj web pretraživača tako da bi hakeru otežali otkrivanje i iskorišćavanje ranjivosti aplikacija web pretraživača
   b. ograničiti broj *web* pretraživača (1–2) da biste bolje ažurirali aplikacije
   c. uvesti pristup Internetu preko modema i zbuniti hakere brojem fizičkih veza
   d. smanjiti broj fizičkih veza sa Internetom uklanjanjem svih modemskih veza
4. Virusni napad:
   a. vrši se uglavnom od klijenta i komunikacije sa serverom bez autentifikacije
   b. omogućava neovlašćeni pristup podacima uz pomoć otkrivene lozinke
   c. uništava podatke
   d. omogućava otkrivanje podataka na bazi šifrata i otkrivenog tajnog ključa
   e. onemogućava funkcionisanja mrežnih servisa i resursa
5. Ukidanja servisa (DoS):
   a. neovlašćeno pristupanje podacima u otvorenom obliku i lozinkama
   b. omogućava otkrivanje podataka na bazi šifrata i otkrivenog tajnog ključa
   c. onemogućava funkcionisanja mrežnih servisa i resursa
   d. omogućava neautorizovani pristup podacima prevarom legalnog korisnika
6. Ponavljanje poslatih poruka:
   a. vrši se uglavnom od klijenta i komunikacije sa serverom bez autentifikacije
   b. omogućava neovlašćena kontrola komunikacije subjekata i ponavljanje, izmena ili sprečavanje prenosa podataka
   c. omogućava otkrivanje podataka na bazi šifrata i otkrivenog tajnog ključa
   d. omogućava neautorizovani pristup podacima prevarom legalnog korisnika
7. Pogađanje lozinke:
   a. vrši se uglavnom od klijenta i komunikacije sa serverom bez autentifikacije
   b. neovlašćeno pristupanje podacima u otvorenom obliku i lozinkama
   c. omogućava neovlašćeni pristup podacima uz pomoć otkrivene lozinke
   d. uništava podatke
   e. omogućava neautorizovani pristup podacima prevarom legalnog korisnika
8. Napad tipa trojanskog konja:
   a. vrši se uglavnom od klijenta i komunikacije sa serverom bez autentifikacije
   b. identifikuje potencijalne objekte napada i locira ranjiva mesta RM
   c. vrši se najčešće prekoračenjem bafera i skriptovanjem preko web lokacije
   d. distribuira zlonamerne programe na radne stanice i krade podatke
   e. neovlašćeno pristupanje podacima u otvorenom obliku i lozinkama
9. Lažno predstavljanje (socijalni inženjering):
   a. identifikuje potencijalne objekte napada i locira ranjiva mesta RM
   b. omogućava otkrivanje podataka na bazi šifrata i otkrivenog tajnog ključa
   c. onemogućava funkcionisanja mrežnih servisa i resursa
   d. omogućava neautorizovani pristup podacima prevarom legalnog korisnika
10. Kriptoanaliza:
   a. vrši se uglavnom od klijenta i komunikacije sa serverom bez autentifikacije
   b. neovlašćeno pristupanje podacima u otvorenom obliku i lozinkama
   c. omogućava otkrivanje podataka na bazi šifrata i otkrivenog tajnog ključa
   d. onemogućava funkcionisanja mrežnih servisa i resursa
   e. omogućava neautorizovani pristup podacima prevarom legalnog korisnika
11. Napad skeniranjem:
   a. vrši se uglavnom od klijenta i komunikacije sa serverom bez autentifikacije
   b. identifikuje potencijalne objekte napada i locira ranjiva mesta RM

c. najčešće prekoračenjem bafera, skriptovanjem preko web lokacije i dr.
d. omogućava neautorizovani pristup podacima prevarom legalnog korisnika

12. Kombinovani napad je:
a. kombinacija više tipova malicioznih kodova
b. slučaj malicioznog kôda koji koristi višestruke metode za širenje
c. kombinacija virusa i trojanaca

13. Tipičan proces napada sadrži sledeće korake:
a. izviđanje, planiranje, dobijanje pristupa i prikrivanje prisustva
b. izviđanje, dobijanje pristupa i prikrivanje prisustva
c. planiranje napada, izviđanje, dobijanje i prikrivanje prisustva

14. Navedite koji su od nabrojanih napada izazvani upotrebom malicioznog kôdu:
a. trojanski konj
b. društveni inženjering
c. virus/crv
d. haker
e. parazitski program

15. Troškovi zloupotrebe IKTS definišu se kao:
a. potreban rad da se analizira, popravi i očisti inficirani sistem
b. gubitak produktivnosti i drugi troškovi otklanjanja posledica napada
c. nabavka AVP, obuka, troškovi osiguranja i troškovi gubitka ugleda

16. Zlonamerni (maliciozni) program je:
a. kôd koji se tajno ubacuje u drugi program sa namerom da se nanese šteta
b. tajni kôd koji se legalno ubacuje u drugi program sa namerom da spreči napad
c. kôd koji se tajno ubacuje u drugi program sa namerom da se unište podaci
d. kôd koji se tajno ubacuje u legalni program sa namerom da se pokrene destruktivni program ili kompromituje bezbednost informacija

17. Osnovne karakteristike virusa su:
a. inficira druge programe, modifikujući ih tako da uključuju njegovu naprednu kopiju
b. samoumnožavaju se, zasebni su programi i ne zavise od izvršnog kôda
c. replicira se, pravi svoje kopije i distribuira ih u druge datoteke ili računare
d. sadrži metode za upad i širenje, algoritam za izbor mete i metod za pretraživanje i *teret za napad*
e. samoumnožavanje u postojeći izvršni kôd je ključni faktor za definisanje
f. pravi se modularno da lakše može promeniti funkcionalnost

18. Osnovne karakteristike crva su:
a. samoumnožavaju se, zasebni su programi i ne zavise od izvršnog kôda
b. replicira se, pravi svoje kopije i distribuira ih u druge datoteke ili računare
c. sadrži metode za upad i širenje, algoritam za izbor mete i metod za pretraživanje i *teret* za napad
d. samoumnožavanje u postojeći izvršni kôd je ključni faktor za definisanje
e. pravi se modularno da lakše može promeniti funkcionalnost

19. Osnovne karakteristike trojanca su:
a. sadrži *serversku* i *klijentsku* komponentu
b. svaki mehanizam, koji zaobilazi normalnu kontrolu pristupa u sistemu
c. pasivno sakuplja informacije sa računara korisnika i šalje ih napadaču
d. sadrži *teret,* koji izvršava neki maliciozni kôd i *okidač*

20. Zadnja vrata su:
a. sadrži *serversku* i *klijentsku* komponentu
b. svaki mehanizam, koji zaobilazi normalnu kontrolu pristupa u sistemu
c. omogućava zaobilazni pristup računaru i eskalaciju lokalnih privilegija
d. sadrži *teret,* koji izvršava neki maliciozni kôd i *okidač*

21. Špijunski program je:
a. sadrži *serversku* i *klijentsku* komponentu
b. svaki mehanizam, koji zaobilazi normalnu kontrolu pristupa u sistemu

c. pasivno sakuplja informacije sa računara korisnika i šalje ih napadaču
b. sadrži *teret,* koji izvršava neki maliciozni kôd i *okidač*

22. Logička bomba:
    a. sadrži *serversku* i *klijentsku* komponentu
    b. omogućava zaobilazni pristup računaru i eskalaciju lokalnih privilegija
    c. sadrži *teret,* koji izvršava neki maliciozni kôd i *okidač*
23. Mobilni kôdovi su:
    a. pasivno sakuplja informacije sa računara korisnika i šalje ih napadaču
    b. aktivni program koji se prenosi sa udaljenog sistema na lokalni i na njemu izvršava bez instrukcije korisnika
    c. sadrži *teret,* koji izvršava neki maliciozni kôd i *okidač*
24. Metodi skrivanja malicioznih programa su:
    a. antiforenzičke tehnike, samozaštita od detekcije i ometanje funkcionisanja
    b. kriptozaštita, samozaštita od detekcije i ometanje funkcionisanja
    c. polimorfizam, metamorfoza, šifrovanje kôda i maskiranje,
    d. tehnike skrivanja (rutkit) i tehnika deaktivacije AVP
25. Distribuciju malicioznih programa omogućavaju:
    a. iskoristive ranjivosti RS/RM, *spam* i zaražene e–*mail* datoteke
    b. programski bagovi i maliciozni skriptovi
    c. zastrašivanje *(Scareware)* i socijalni inženjering
    d. *Peer–to–peer* mreže, USB uređaji, optički mediji i hardver
    e. mobilni telefoni i Wi–Fi uređaji
26. Mere zaštite i oporavak od malicioznih programa:
    a. višeslojna antivirusna zaštita, nadzor i kontrola log tragova
    b. fizička AC, politika zaštite i blokiranje sadržaja
    c. zaštita IP adresa servera i korišćenje smart
    d. restauraciju integriteta sistema iz rezervne kopije
27. Ključni kriterijumi za procenu napada u analizi rizika su:
    a. posledica uticaja, lokacija izvora i način izvođenja
    b. intenzitet uticaja, izvor nastanka i način izvođenja
    c. posledica uticaja, izvor nastanka i način izvođenja
    d. posledica uticaja, izvor nastanka i primenjena tehnika napada

8. TEHNOLOGIJE ZA ZAŠTITU RAČUNARSKIH SISTEMA

Po završetku ovog poglavlja razumećete:

- Značaj tehnologije u sistemu zaštite RS i RM
- Opštu podelu alata (mehanizama i protokola) za zaštitu
- Osnovne alate za zaštitu RS
- Koncept višeslojne zaštite

8.1. UVOD

Proceduralne i *tehničke* kontrole zaštite mogu se smatrati različitim aspektima jednog rešenja sistema zaštite. Obično nema smisla birati tehničke mehanizme zaštite bez proceduralnih rešenja, kao i što procese zaštite treba projektovati prema tehnološkim mogućnostima i raspoloživim alatima da bi se obezbedio željeni nivo podrške tom procesu. Drugim rečima, *samo kombinacijom tehnika, alata i proceduralnih kontrola ostvaruje se efektivna arhitektura sistema zaštite*.

Generička arhitektura sistema zaštite obuhvata najveći skup poznatih i dostupnih proceduralnih i tehnoloških komponenti zaštite, koje se menjaju u zavisnosti od specifičnosti IKTS, bezbednosnih zahteva i procene rizika u konkretnoj organizaciji. Definisanje arhitekture sistema zaštite sugeriše se u početnoj fazi razvoja životnog ciklusa IKTS, a u fazi projektovanja, arhitektura sistema zaštite se doteruje u skladu sa rezultatima procene rizika, mogućnostima i potrebama organizacije.

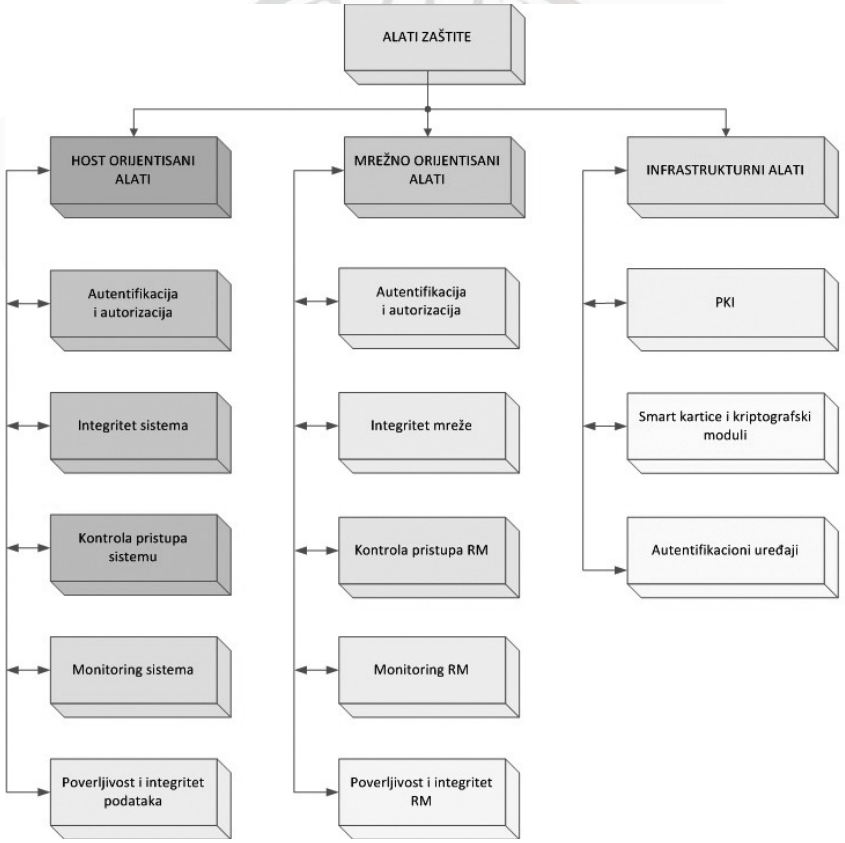
U opštem slučaju, tehnike i alati zaštite mogu se podeliti na *host orijentisane* (na RS) i *mrežno orijentisane* (na RM). Za upravljanje alatima zaštite RS/RM, potrebno je obezbediti određene kontrolne strukture – *kontrole zaštite***.**

8.2. KLASIFIKACIJA ALATA ZA ZAŠTITU

Klasa host–orijentisanih alata za zaštitu, namenjena je za poboljšanje NOSSS zaštite servera, radne stanice, aplikacija i podataka. *Klasa mrežno orijentisanih alata* odnosi se na mehanizme i protokole za zaštitu RM. *Klasu alata za infrastrukturnu podršku* čine kompleksni, infrastrukturni alati za zaštitu i veću funkcionalnu podršku IKTS. U odnosu na tipove *servisa zaštite* koje podržavaju i realizuju, unutar prve dve klase, alati zaštite se dalje klasifikuju na alate za: *identifikaciju, autentifikaciju i autorizaciju (RS/RM), zaštitu integriteta (RS/RM), kontrolu pristupa (RS/RM), monitoring sistema zaštite (RS/RM) i zaštitu poverljivosti, integriteta i raspoloživosti podataka i informacija.*

Sa aspekta OOM, prva četiri servisa gledaju na RS/RM kao na *kontejnere* informacija i namenjeni su za zaštitu tih kontejnera, dok poslednji servisi direktno štite poverljivost, integritet i raspoloživost informacija u RS/RM. Važno je razumeti razliku između integriteta RS/RM i integriteta podataka. Zaštita integriteta RS usmerena je na detekciju i potencijalno sprečavanje i oporavak od maliciozne modifikacije komponenti sistema, dok je zaštita integriteta RM namenjena da obezbedi celovitost konfiguracije RM. Na primer, mehanizmi za zaštitu integriteta RM mogu otkriti prisustvo neovlašćene mašine povezane na RM. Mehanizmi za zaštitu integriteta podataka namenjeni su za zaštitu nepromenljivosti podataka. Primer je protokol zaštite koji detektuje promene na podacima u toku prenosa.

Za klasifikaciju tehničkih alata zaštite, primenjuje se *objektno–orijentisana* šema (Sl. 8.1) [74].



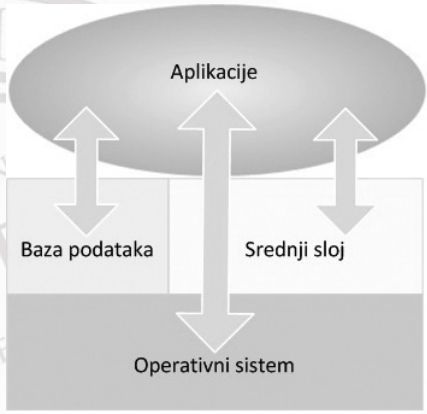
Sl. 8.1. Klasifikacija alata za zaštitu

8.3. MEHANIZMI ZAŠTITE RAČUNARSKOG SISTEMA

8.3.1. Apstraktni bezbednosni slojevi računarskog sistema

Za definisanje *slojeva zaštite u RS* koristi se slojevita struktura apstraktnih nivoa u RS, slično OSI modelu arhitekture RM. Dakle, osnovni *koncept slojevite zaštita* počinje već u samom RS. Uprošćeni model (Sl. 8.2) se koristi samo za ilustrovanje osnovnog koncepta zaštite RS. *Operativni sistem* (OS), najznačajniji apstraktni sloj RS, učestvuje u svim zadacima koje RS obavlja. Zato, *zaštita OS određuje najviši nivo zaštite celog IKTS*. Naime, ako se OS kompromituje, samo je pitanje vremena kada će ceo RS biti kompromitovan, pre svega sloj aplikacija koji komunicira direktno sa OS [74, 85].

Baze podataka i *srednji sloj* (*middleware*) su sistemski programi za podršku OS, dok sloj aplikacija direktno pristupa OS. Sistemski programi za podršku OS obezbeđuju određene standardne servise za brojni skup aplikacija. Osnovni koncept je da viši sloj programa prima neku vrstu servisa od nižeg sloja. Primeri ovih programa su *relacione baze podataka* i arhitektura *middleware* (*brokera* zahteva za zajedničke objekte). Pošto ovi programi koriste servise, koje nudi OS, njihova zaštita je nužno zavisna od zaštite OS i ako je OS probijen preko sloja aplikacija, lako je zaobići mehanizme zaštite baze podataka i *middleware* sloja.



Sl. 8.2. Apstraktni bezbednosni slojevi RS

Primer 1: Relacionu bazu štiti servis kontrole pristupa i nalog administratora. Ako se na neki način dobije nalog superkorisnika, onda je lako dobiti pristup bazi podataka. Takođe, zaštita aplikativnog sloja je zavisna od zaštite oba donja sloja.

Primer 2: Za zaštitu baze podataka koristi se kriptozaštitni mehanizam, koji mora ispuniti stroge zahteve čuvanju kriptoloških ključeva u uređaju otpornom na proboj (*smart* kartica), da bi se sprečio privilegovan korisnik da izvuče ključeve, koristeći uslužne alate. Dizajn arhitekture treba da spreči da se podaci nikada ne pojavljuju u otvorenom tekstu u memoriji RS ili sekundarnim memorijama (USB, CD, ..). Interfejs između OS i uređaja za skladištenje kriptoloških ključeva treba da bude zaštićen sa protokolom zaštite, da neovlašćeni korisnik sa privilegovanim pravima, ne može prisluškivati razmenu između baze podataka i uređaja i posle toga preko interfejsa ući u sistem. Dakle, ko kontroliše OS obično kontroliše sve što je aktivno iznad OS. Zato dobar sistem zaštite počinje sa dobrom zaštitom OS.

8.3.2. Podsistem za zaštitu OS (NOSSS)

Jedan od čvrstih stereotipova među specijalistima zaštite je tretiranje (pod)sistema zaštite OS – NOSSS, kao *dominantne komponente zaštite*. Na zaštitu OS izdvajaju se znatna sredstva na račun ostalih komponenti realnog sistema zaštite. Međutim, u savremenim IKTS sa višeslojnom arhitekturom klijent – server tipa, OS ne kontroliše sve *objekte* sa kojima korisnici rade, kao ni aktivnosti samih korisnika, koji svoj pristup OS-u registruju mehanizmima za kontrolu pristupa. Na taj način, osnovna bezbednosna funkcija NOSSS postaje samo *zaštita prava privilegovanih* korisnika (administratora, supervizora i dr.) *od napada regularnih korisnika* (interno zaposlenih), što je značajno, ali nedovoljno za bezbednost IKTS. Takođe, u sistemu zaštite, rentabilnom i sinhronizovanom sa životnim ciklusom IKTS, jednako su značajne proceduralne i tehničke kontrole, kao i povećanje efikasnosti i efektivnosti procesa upravljanja zaštitom [61].

Kako je NOSSS osnovni sloj zaštite svih programa u RS, dobro je da drugi tipovi zaštite budu kompatibilni sa zahtevima NOSSS, a ne obrnuto. U razvoju *strategije* zaštite, treba jačati zaštitu komplementarnu NOSSS, dodavanjem drugih tipova zaštite, vodeći računa da ti mehanizmi ne budu u konfliktu sa NOSSS alatima. Karakteristike NOSSS alata za zaštitu prilično su standardne i obično uključuju osnovne mehanizme, kao što su *mehanizmi kontrole pristupa* i *autentifikacije korisnika* operativnom sistemu i mehanizmi *logovanja bezbednosno relevantnih događaja*. Načini implementacije ovih mehanizama zavise od vrste platforme, pa je teško definisati homogene zahteve. Glavna opasnost od upotrebe univerzalnih programa za zaštitu, je udaljavanje korisnika od NOSSS mehanizama i korišćenje za zaštitu heterogenih platformi. Administrator zaštite obično isključe NOSSS zaštitu, a da pri tome dodatni program za zaštitu uopšte ne podržava neku funkciju zaštite NOSSS.

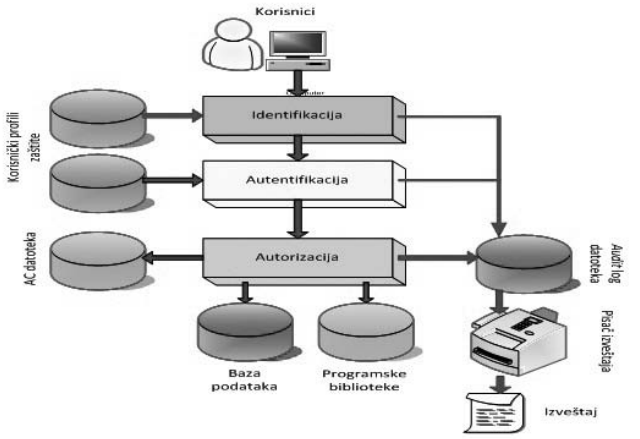
Iako ni jedan OS nikada neće biti potpuno zaštićen, neki TTP nude *poverljive OS* zasnovane na kriterijumima evaluacije poverljivih računarskih sistema – TCSEC (*Tusted Computer System Evaluation Criteria*). Za korišćenje TCSEC treba poznavati kriterijume prema kojima je sistem evaluiran i tip rizika kojeg otklanja. Korišćenje TCSEC programa za ekstra zaštitu, često smanjuje funkcionalnosti, tako da se neke aplikacije uopšte ne mogu izvršavati [84].

Microsoft neprekidno poboljšava bezbednost svojih OS, još od Windows NT 4.0. NOSSS OS Windows 7, uključuje sistem za šifrovanje fajlova – **EFS** (*Encrypting File System*), koji podržava kriptološki algoritam – **ECC** (*Elliptic Curve Cryptography*), pogodniji mehanizam za kontrolu pristupa i poboljšani mehanizam za kontrolu aplikacija, koje se mogu instalirati na korisnički računar – **AppLocker**. Takođe, uvedeni su novi koncept **DirectAccess**, koji bezbedno spaja legitimnog udaljenog korisnika na IKTS organizacije i **BitLocker,** koji šifruje podatke na nivou bita.

8.3.3. Logička kontrola pristupa računarskom sistemu

Logička kontrola pristupa – **LAC** (*Logical Access Control*) je servis za upravljanje pravilima, prema kojima korisnici mogu ostvariti logički pristup objektima IKTS. Razlikuju se softverski *mehanizmi za AC* RS (*mainfraim tipa)*, koje uključuje NOSSS većine savremenih OS i *univerzalna rešenja* za kontrolu pristupa različitim platformama i centralizovanu administraciju više korisnika – **EUA** (*Enterprise User Administration*), koji mogu raditi sa postojećim NOSSS na većini platformi.

Generički servis LAC (Sl. 8.3) uključuje mehanizme za *identifikaciju, autentifikaciju i autorizaciju* legitimnih korisnika OS–u računara, koji se koriste za restrikciju pristupa objektima RS [61].



Sl. 8.3. Generički servis logičke kontrole pristupa

Korisnik se *identifikuje* sistemu sa *korisničkim imenom,* a *identitet verifikuje* (*autentifikuje)* nekim *identifikatorom*, koji može biti nešto što *ima* (kartica sa PIN), *zna* (lozinka) ili što stvarno *jeste* (biometrijski parametar). Pošto većina korisnika danas pristup IKTS preko lokalne mreže ili udaljenim pristupom preko Interneta, autentifikacija korisnika se smatra mrežnim procesom. Standardni mehanizmi za autentifikaciju su *autentifikacioni protokoli i uređaji (serveri, smart kartice)*.

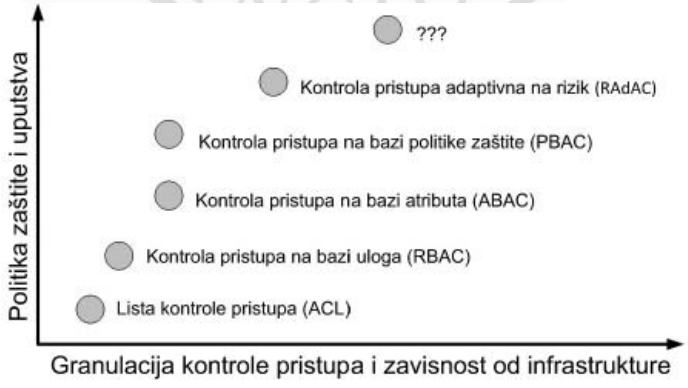
U savremenim RS, za autentifikaciju korisnika OS–u, najviše se primenjuju *korisničko ime i lozinka*. U praksi se vrlo često koriste iste lozinke za različite aplikacije, što je kršenje politika zaštite, jer se povećava mogućnost proboja rečničkim napadom. Rezultati istraživanja korisničke upotrebe i upravljanja lozinkom (Tabela 8.1) pokazali su da oko 77% ispitanih koristi istu lozinku za različite aplikacije [23]. *Autorizacija* je proces dodeljivanja legalnim korisnicima prava pristupa i aktivnosti na objektima RS.

Tabela 8.1. Statistika korisničke upotrebe lozinke

Upotreba lozinki						
Ne koriste		Od 1–3		Od 4–10		Više od 10
10%		11%		29%		50%
Tipična dužina lozinke						
Zavisno od potrebe		8 i više karaktera		6–8 karaktera		1–5 karaktera
29%		44%		28%		3%
Zaboravljanje lozinke						
Ne koriste lozinku	Nikad (zapisuje)	Jednu nedeljno	Nikad (pamti)	Jednom mesečno	Nikad (menadžer lozinki)	Jednom godišnje
2%	5%	8%	16%	17%	26%	26%

8.3.3.1. Mehanizmi logičke kontrole pristupa

Generički servis LAC evoluirao je od *obavezne* **– MAC** (*Mandatory Access Control*), na osnovu utvrđenih pravila, primarno primenjivane u državnim organizacijama (vojska, policija) i *diskrecione* **– DAC** (*Descretionary Access Control*), na osnovu odluke vlasnika sistema u poslovnim sistemima, do svaremenih modela kontrole pristupa na bazi sledećih mehanizama: *liste kontrole pristupa* (ACL), *uloga* (RBAC), *atributa* (ABAC), *politike zaštite* (PBAC) i *adaptivnih na rizik* (RadAC), (Sl. 8.4) [62].



Sl. 8.4. Mehanizmi logičke kontrole pristupa [62]

Lista kontrole pristupa (ACL) je osnovna forma LAC, nastala 1970–ih zbog potrebe ograničavanja pristupa više korisnika deljenim resursima UNIX *mainframe* sistema. ACL je fokusirana na resurse RS/RM, gde se politika pristupa podešava za svakog korisnika i koriste je brojni OS (Unix, Windows, Linux). Koncept ACL je jednostavan – svaki resurs sistema, kojem treba kontrolisati pristup, predstavlja objekat sa pridruženom listom prava pristupa i aktivnosti entiteta na tim objektima. ACL se može primeniti na pojedinačnu datoteku, direktorijum ili grupu procesa i često obezbeđuje dovoljno privilegija za modifikaciju liste. ACL se može koristiti u kontekstu RM, gde se zahteva udaljeni pristup, kao i u sistemima za upravljanje relacionom bazom podataka i nekim aplikacijama. Osnovni nedostaci ACL su slaba efikasnost, jer se mora proveravati svaki put kad korisnik pristupa resursu, teško upravljanje sa velikim brojem korisnika i prava pristupa na različitim nivoima i neprihvatljivo vremenski zahtevne i sklone greškama modifikacija.

Kontrola pristupa na bazi uloga u organizaciji (RBAC) je noviji metod u kojem se pristup resursima RS/RM određuje na bazi uloga korisnika u organizaciji. RBAC otklanja neke nedostatke ACL i pruža nove mogućnosti LAC – određuje pristup na bazi uloge korisnika, nezavisno od tipa resursa kojem pristupa. RBAC omogućava grupisanje korisnika, pa se politika pristupa podešava samo jedan put za određeni resurs i grupu korisnika. Omogućava da korisnici budu članovi više grupa, npr. član jedne grupe sa određenim pravima i posebnim privilegijama druge grupe (npr. supervizor). Ako su privilegije u konfliktu, pristup zavisi od OS i prioriteta privilegija u konkretnom slučaju. *Privilegovani nalog* obezbeđuje administratoru sistema da određenim korisnicima daje na kontrolisan način mogućnost da koriste neke selektivne komande pod administratorskim nalogom, a da pri tome ne deli svoj nalog sa tim korisnicima. Privilegovani menadžerski nalog se koristi da obezbedi zaštitu OS, a ne rad sa programima za podršku ili sa slojem aplikacija.

U poslovnim sistemima najčešće se koristi RBAC metod, gde se korisnici dodaju ili uklanjaju iz grupe u procesu administracije LAC servisa. Varijante RBAC metoda su implementirane na različitim nivoima u većini savremenih OS, npr. Windows 2000 i kasnije verzije uvele su grupe korisnika: *administrator*, *privilegovani korisnici* i *korisnici*. RBAC se sve više primenjuje na nivou aplikacija, obično kao komponenta srednjeg sloja. Na primer, *IBM Tivoli Identity Manager* ima RBAC komponentu koja tretira ulogu korisnika kao deo njegovog identiteta. Osnovni nedostatak RBAC metoda LAC je problem definisanja veće granulacije prava pristupa za svakog korisnika, što je često potrebno [41].

Kontrola pristupa na bazi atributa korisnika (ABAC) je metod LAC gde se odluka o kontroli pristupa donosi na bazi seta karakteristika ili atributa entiteta koji zahteva pristup sistemu direktno ili posredno. Korisnik se identifikuje sistemu setom atributa, koji se porede sa referentnim atributima u bazi podataka, a sistem dopušta/odbija pristup zavisno od politike LAC. Ključna prednost ABAC metoda je što nije potrebno da korisnik, koji pristupa sistemu/resursu, bude unapred poznat. Ako atributi korisnika odgovaraju kriterijumima za davanje prava pristupa, pristup će biti dodeljen. Ovaj metod nije dobar za velike organizacije u kojima korisnici mogu po volji pristupiti/napustiti organizaciju i gde ima mnogo resursa, korisnika i aplikacija sa različitim atributima, koje je potrebno

harmonizovati. Većina savremenih OS ne podržava podrazumevano ABAC metod kontrole pristupa.

Kontrola pristupa na bazi politike zaštite (PBAC) određuje specifičnim izjavama, ko i pod kojim uslovima može imati pristup određenim resursima. Takođe, navodi se mehanizam implementacije, čime se uspostavlja kontrola i odgovornost menadžerske strukture. PBAC metod je u razvoju i predstavlja harmonizaciju i standardizaciju ABAC metoda, koji uključuje atribute za pristup određenom resursu na lokalnom nivou. PBAC zahteva mnogo kompleksniju logiku, jer kombinuje atribute resursa, okruženja i korisnika koji zahteva pristup, sa informacijama o uslovima pod kojim se pristup odobrava. Primer politike LAC u mašinski čitljivom formatu je **XACML** (*The eXtensible Access Control Markup Language*) baziran na XML–u.

Metod kontrole pristupa adaptivne na rizik (RAdAC) obezbeđuje LAC u realnom vremenu, koja se prilagođava dinamičkoj promeni faktora rizika. Ovaj metod predstavlja suštinski pomak od ostalih načina LAC i, pored koncepta operativnih potreba, uvodi uslove okruženja i nivoe rizika u proces odlučivanja mehanizma za LAC. RAdAC se, za kreiranje kvantitativne metrike rizika, ne oslanja samo na tradicionalne atribute i politike, nego kombinuje informacije o poverljivosti lica (mašina), IKT infrastrukturi i faktorima rizika okruženja. Takođe, koristi situacione faktore kao ulaze u proces odlučivanja mehanizma, koji mogu uključivati informacije o tekućem nivou pretnji, dobijene iz drugih izvora (CERT, proizvođač).

8.3.3.2. Univerzalni mehanizmi logičke kontrole pristupa

Univerzalni EUA softverski mehanizmi centralizuju upravljanje LAC servisom u distribuiranom okruženju. Nasuprot *mainframe* mehanizmu za LAC velikom broju OS, baza podataka i aplikacija, sa sopstvenim modelima zaštite, EUA rešava brojne probleme *pregleda LAC podataka iz više mašina, kotrole promena na korisničkim nalozima i pravima pristupa na svakom RS i kretanja administratora od jednog do drugog tipa RS.* EUA program zahteva poznavanja svake platforme, obezbeđuje interfejs za upravljanje različitim LAC mehanizama, ali ih direktno ne implementira u OS. EUA LAC je neefikasna za autorizaciju sa niskim nivoom automatizacije.

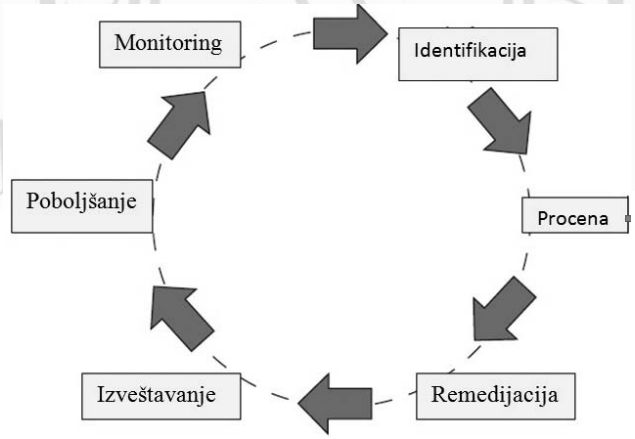
Najčešće rešenje arhitekture EUA programa slično je onom kojeg koriste *host* orijentisani skeneri zaštite, a uključuje *softverskog agenta,* koji radi na ciljnoj platformi, *upravljačku aplikaciju,* koja može komunicirati sa agentom i softver *korisničkog interfejsa*. Upravljanje (kreiranje, modifikacija ili ukidanje) naloga korisnika može se vršiti direktno na ciljnoj platformi ili preko jedne tačke (administracije) u EUA. Konzistentnost centralne baze podataka koju održava EUA sistem, obezbeđuje se dijalogom između EUA agenta i upravljačke aplikacije. Proces sinhronizacije ovog dijaloga razlikuje se od proizvoda do proizvoda i može uključivati sinhronizaciju u realnom vremenu ili pomoću *batch* procesa, u kojem se skup programa izvršava u računaru u isto vreme, ali u tom

slučaju postoji „*prozor rizika*" (bez sinhronizacije), što može dovesti do pogrešne odluke administratora.

Softverski agent je aplikacija, koja radi na vrhu NOSSS na ciljnoj platformi ili kao eksterni softver za LAC, u *mainframe* OS. Neki paketi nude API (*Application Programming Interface*), koji podržava autorske aplikacije. Jedna posledica primene udaljenog agenta je, da ne podržava sve funkcionalnosti originalnog OS, što može stvoriti ranjivost za obaranje sistema. Veza između centralno upravljanog sistema i agenta obično se šifruje, da se spreči modifikacija podataka u prenosu. Alternativni pristup korišćenju EUA programa je adaptacija meta–baze podataka (*Data Warehous*) za centralizaciju podataka LAC servisa. Ovo rešenje, međutim, ne razmenjuje bezbednosno relevantne podatke sa drugim entitetima i ne obezbeđuje integraciju sa postojećim sistemima, kao EUA program [74].

8.3.4. Zaštita integriteta računarskog sistema

Definicija *ranjivosti* uključuje *softversku*, *hardversku* i *grešku konfiguracije,* koju može iskoristiti maliciozni napadač. *Upravljanje ranjivostima* podrazumeva upravljanje popravkama, konfiguracijom i zaštitom informacija (Sl. 8.5).



Sl. 8.5. Faze procesa upravljanja ranjivostima

Postoje dve kategorije ranjivosti u Windows platformama: *nepoznati prozor ranjivosti* – od vremena otkrivanja ranjivosti do popravke sistema i *poznati prozor ranjivosti* – od vremena objavljivanja popravke do remedijacije sistema. U Tabeli 8.2. prikazan je primer proračuna prozora poznatih ranjivosti.

Tabela 8.2. Primer proračuna prozora poznatih ranjivosti

Ranjivost	Vreme izveštaja snabdevaču softvera	Vreme objavljivanja popravke	Delta vreme	Vreme popravke /ublažavanja rizika
IE, CVE*–2006–1359 (ranjivost teksta)	10.02.2006	11.04.2006	60 dana	
CVE–2006–0058 (brzina slanja e–pošte)	1.01.2006	22.03.2006	9 dana	
CVE–2005–11–17 (preplavljivanje *QuickTime QTS*)	17.11.2005	10.01.2006	54 dana	
CVE–2006–0006 (preplavljivanje BMP *MediaPlayer*)	17.10.2005	14.02.2006	120 dana	

* CVA (*Common Vulnarability and Exposures*) – uobičajene ranjivosti i izlaganja

Za upravljanje ranjivostima većina organizacija je prepuštena snabdevačima, a u nekim slučajevima licima/entitetima (CIRT/CERT), koji objavljuju/otkrivaju nove ranjivosti. Korisnici mogu brojnim alatima ažurno pratiti bezbednosne ranjivosti i popravke sistemskih programa. Na primer, većina snabdevača nude e–*mail* liste ranjivosti: *Bugtraq* (www.securityfocus.com/archive/ 1/description), originalnu listu bezbednosnih ranjivosti; *VulnWatch* (www. vulnwatch.org, uporedivu sa *Bugtraq,* ali slabije posećivanu; *MS Security Bulletins* (www.microsoft.com) listu ranjivosti MS proizvoda itd. [60].

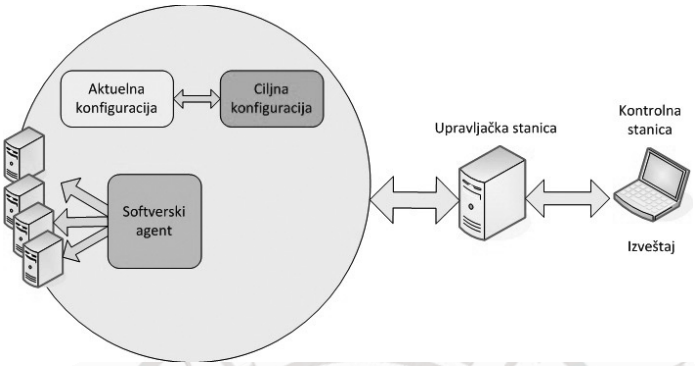
Integritet sistema kontrolišu *skeneri*, koji se dele na *skenere RS* i *skenere RM*.

Skeneri integriteta računarskog sistema rade na principu periodičnog monitorisanja aktuelne konfiguracije platforme na sve tipove ranjivosti. Ranjivost se skenira poređenjem tekuće konfiguracije sa predefinisanom, idealnom konfiguracijom za datu platformu. Iako skeneri integriteta mogu raditi na svim apstraktnim nivoima, u praksi su retki na aplikativnom nivou, pošto zahtevaju detaljno poznavanje skenirane aplikacije. U praksi glavna je upotreba skenera ranjivosti samog OS.

Skeneri ranjivosti OS uglavnom se koriste u okruženju IKTS manjeg obima, pošto bezbednost ovih sistema obično zavisi od korektnosti podešavanja velikog broja opcija konfiguracije. Zavisno od OS moguće je uskladištiti datoteku osnovne i druge konfiguracije na brojne lokacije u sistemu, pa im je teško manuelno pratiti trag. Nažalost male promene u većini ovih opcija mogu imati drastičan uticaj na ukupan nivo zaštite sistema, a te se promene mogu dogoditi zbog *ljudske greške* (npr. rad administratora pod pritiskom), *neznanja* (npr. omogućen servis za daljinski pristup) i zbog *instalacije novog programa*. U IKTS srednjeg i velikog obima, nije moguće upravljati ovolikom kompleksnošću bez automatizovanih alata.

Tipična implementacija skenera obuhvata *softverskog agenta,* koji skenira niz ciljnih platformi i verifikuje aktuelnu konfiguraciju u odnosu na ciljnu, *upravljačku stanicu,*

koja skuplja podatke sa svih skeniranih platformi u RM i *kontrolnu stanicu,* koja koristi *korisnički interfejs* za generisanje izveštaja. Na Sl. 8.6. ilustrovana je upotreba skenera ranjivosti većih IKTS.



Sl. 8.6. Primena skenera ranjivosti u IKTS srednje veličine

Administrator koristi klijentski interfejs za pristup rezultatima skeniranja. Softverski agent je obično specifičan za OS i dolazi sa prekonfigurisanom bazom podataka uobičajenih ranjivosti OS i predefinisane politike. Ovi predefinisani parametri koriste se kao početne vrednosti za definisanje osnovne zaštite i politike skeniranja za specifičnu lokaciju. Vendori obično nude ažuriranje softvera za skeniranje. Ovi alati mogu imati dodatne funkcionalnosti, kao što su zaštita lozinkom i mogućnost monitorisanja promene sadržaja (npr. skladištenjem sažetaka datoteka – *heš vrednosti*). Alati za skeniranje poznatih ranjivosti hosta mogu se naći na *web-u* [101].

Komercijalni skeneri zaštite mogu prezentovati otkrivena odstupanja od ciljne konfiguracije u formi izveštaja i grafičkog prikaza. Neki alati imaju mogućnost automatske korekcije stanja, što je delikatna operacija, jer korekcija ranjivosti sistema zaštite može imati veliki uticaj na funkcionisanje sistema. Ključno pitanje o efektivnosti skenera ranjivosti je u kojoj meri redukuju rizik, što zavisi od dva faktora – *mere u kojoj osnovna konfiguracija zaštite odražava željeni profil rizika i efikasnosti procesa korekcije, koji sledi nakon otkrivanja ranjivosti*. Ako su ova dva faktora korektno upravljana, skeneri ranjivosti mogu obezbediti više dodatnih kontrola u distribuiranom IKTS.

Antivirusni programi (AVP) otkrivaju i uklanjaju kompjuterske viruse i druge maliciozne programe, koji menjaju integritet RS, pošto se instaliraju na lokalnoj platformi, a zatim je koriste za dalju propagaciju u RM. Koncept AVP je jednostavan. Svaki put kada AVP otkrije maliciozni kôd, u cilju identifikacije ispituje deo strukture osoben za taj kôd, što su najčešće heš vrednost ili digitalni potpis. Ovaj elemenat strukture je *definicija* ili *potpis* malicioznog kôda, koja se preuzima ažuriranjem baze podataka AVP, a kasnije koristiti za detekciju prisustva poznatih malicioznih kôdova. AVP jednostavno radi tako što

skenira OS, baze podataka i aplikacije, tražeći potpise malicioznih kôdova uskladištenih u bazi definicija AVP. Kada otkrije maliciozni kôd sa poznatom definicijom, u AVP se aktivira set instrukcija za uklanjanje te definicije.

U stvarnosti zadatak AVP mnogo je složeniji, pošto autori malicioznih kôdova nalaze brojne načine da poraze ovaj jednostavni odbrambeni mehanizam. Neki virusi koriste tehnike kriptozaštite za skrivanje potpisa malicioznih kôdova. Zbog toga su savremeni AVP dizajnirani tako da rade i na aplikativnom sloju i sloju OS i da mogu skenirati veliki obim objekata, kao što su memorije, datoteke, e-pošta i dodaci i but sektori. Osim toga, skeniranje AVP nije ograničeno na jednostavnu detekciju definicija malicioznih kôdova, nego može uključivati napredne tehnike kao što su dešifrovanje i uklanjanje u izolovan prostor (karantin).

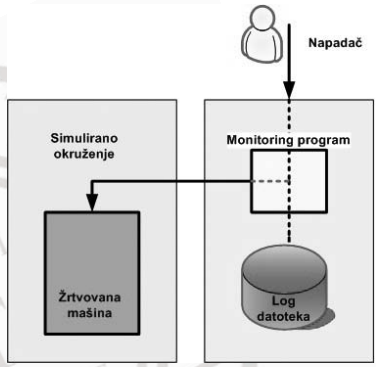
Skeneri sadržaja i filteri e-pošte mogu analizirati sadržaj preuzetih mobilnih kôdova ili poruka e-pošte, detektovati potencijalne povrede sistema zaštite i izvršiti akciju odgovora na pretnje. Ove funkcionalnosti su korisne za zaštitu integriteta OS. Iste tehnike mogu se koristiti i za zaštitu integriteta podataka. Na primer, legalni korisnik razmenjuje pornografski materijal sa serijom kontakata izvan organizacije. To radi *steganografskom* ugradnjom slike ili teksta u poruke e-pošte. Skeneri sadržaja mogu detektovati ugrađene slike ili tekst i smestiti ih u karantin za dalju analizu. U ovom primeru, softveri skenera sadržaja direktno se koriste za zaštitu samih podataka.

Skeneri sadržaja su komplementarni AVP-a. Rade na aplikativnom nivou, pošto obično ispituju informacione objekte koji su u prenosu između dva sistema. Ovaj pristup je potencijalno moćniji od AVP detekcije bazirane na potpisu, zato što se mogu ugraditi pravila bazirana na različitim kriterijumima i nisu ograničeni na, u suštini, statička svojstava objekata malicioznih kôdova. Programi za filtriranje sadržaja mnogo variraju po obimu i sofistikaciji. Kreću se od jednostavnih skenera sadržaja e-pošte, koji vrše leksičku analizu i odlažu u karantin poruke koje sadrže određene, predefinisane reči/fraze, do sofisticiranih skenera sadržaja koji u realnom vremenu ispituju dolazne poruke i preuzete sadržaje sa Interneta. Ovo je posebno značajno za bezbednosnu proveru prisustva mobilnih kôdova (*Java, JavaSkript i ActiveX)*.

Većina skenera sadržaja obezbeđuje nekoliko načina reagovanja na povredu politike zaštite i omogućava administratoru da konfiguriše odgovarajuće akcije na bazi tih pravila. U slučaju e-pošte, skeneri sadržaja mogu odlagati u karantin ili izbrisati dodatke sa porukama ili odbaciti poruku u celini u *junk* direktorijum. Skeneri sadržaja mobilnih kôdova mogu blokirati preuzeti sadržaj, preneti sumnjivi sadržaj TTPS provajderu na analizu, izvršiti logovanje i potencijalno poslati alarm korisniku. Neki *web* filteri mogu prepoznati i odgovoriti na sadržaj. Filteri e-pošte imaju ugrađene AVP, a AVP počinju ugrađivati neke od funkcionalnosti skenera sadržaja, što znači da ova dva mehanizma konvergiraju u jedinstven proizvod.

8.3.5. Mehanizmi za detekciju i sprečavanje upada u sistem

Sistemi za detekciju i sprečavanje upada – IDPS (*Intrusion Detection and Protection Systems*) koriste se za prepoznavanje indikacija nekog pokušaja upada, upozorenje korisnika i izvršavanje korektivnih akcija za sprečavanje upada u IKTS [2, 87, 89]. Savremeni koncept IDPS omogućava, pored funkcija detekcije upada (IDS), određenu vrstu inteligentne zamke za napadača (tipa ćupa meda – *hony pot*), kojima skreću njihovu pažnju i za to vreme izučavaju osobenosti u cilju preventivne zaštite i *sprečavanja* sledećeg upada (Sl. 8.7).



Sl. 8.7. IDPS koncept

Postoje dve velike klase IDPS sistema – *IDPS računarskog sistema ili HIDPS i IDPS računarske mreže ili NIDPS.* Oba sistema analiziraju indikatore upada, ali se razlikuju načini na koji to rade i tipovi podataka koje procesiraju. Prednosti i nedostaci su slični onima kod skenera ranjivosti. *IDPS sistemi* se, takođe, mogu klasifikovati prema principima detekcije na *sisteme detekcije na bazi potpisa i složene detektore anomalija*. Prvi upoređuju log datoteku poznatih potpisa napada sa aktuelnim, dok drugi traže anomalije prema obrascima, koje sistemi koriste. HIDPS sistemi mogu koristiti različite mehanizme za detekciju i sprečavanje upada, kao što su pseudorelaciona analiza kontrolnih tragova i provera integriteta datoteka. Neki proizvodi kombinuju mehanizme potpisa i detekciju anomalija i omogućavaju brzo ažuriranje baza potpisa napada. HIDPS programi su obično dizajnirani za određene OS, koji pružaju maksimum funkcionalnosti, kao što su direktna intercepcija i interpretacija pristupnih poziva sistemu. Funkcionalnost HIDPS sistema zavisi od analize kontrolnih tragova u log datototeci, što je i glavna ranjivost zbog mogućnosti proboja i modifikacije njenih podataka. HIDPS sistemi obično rade i sa šifrovanim podacima, koje ciljni host dešifruje pre procesiranja. IDPS sistemi generalno imaju dobre sisteme izveštavanja sa različitim nivoima detalja i grafičkim displejom.

Mehanizmi za upravljanje log datotekama obezbeđuju selektivan pristup log datotekama kontrolnih tragova bezbednosno-relevantnih događaja. U okruženju sa različitim platformama, ovi mehanizmi pomažu osetljivi proces skupljanja i kombinovanja *login* informacija sa različitih platformi, što omogućava praćenje napada ili sumnjivih događaja, koji pogađaju više od jednog hosta. Pošto većina OS obezbeđuje *logovanje*, mehanizmi za upravljanje log datotekama koriste se za zaštitu na svim apstraktnim slojevima RS.

Izvlačenje relevantnih podataka iz *log* datoteka u većim IKTS, veoma je složen i vremenski zahtevan posao. Pre svega, treba razmisliti koje događaje upisivati u *log* datoteke za svaku datu aplikaciju. Ako je ovo učinjeno korektno, za analizu informacija u log datotekama, ostaju problemi *velikog obima podataka i jasnih pravila za proaktivnu i reaktivnu analizu i skladištenje kontrolnih tragova u kontekstu brojnih platformi.* Mehanizmi za upravljanje log datotekama smanjuju problem obima podataka kontrolnih tragova, obezbeđujući filtriranje podataka, na osnovu implementiranog skupa pravila za selekciju. Međutim, ovim se mogu odstraniti važne informacije, pa mehanizmi za upravljanje log datotekama moraju biti inteligentni, da prepoznaju podatke istog tipa na različitim platformama. Takođe, nedostaje standardizacija reprezentacije kontrolnih tragova (cilj projekta *COAST Audit Trail Reduction Group* [16]*)*, koja bi omogućila analizu, a ne interpretaciju sirovih podatka. U log datotekama treba označavati tragove, koji su za proaktivnu ili reaktivnu analizu.

U većini sistema, vreme časovnika različitih platformi približno je sinhronizovano protokolima za automatsku sinhronizaciju (npr. NTP – *Network Sinhronization Protocol)*, koji nisu uvek implementirani u mrežama. Problem sinhronizacije časovnika može uticati na procese konsolidacije hronologije napada, kao i na podatke, koje daju filteri log podataka. Većina savremenih mehanizama samo delimično rešava ove probleme. Brojni alati za analizu *log* datoteka *web* lokacija su sofisticirani, ali ne prate bezbednosne događaje, nego posete klijenata.

8.3.6. Mehanizmi za zaštitu poverljivosti i integriteta podataka

Osnovni mehanizmi za zaštitu poverljivosti i integriteta podataka su *kriptografski hardverski ili softverski mehanizmi*. Kriptografija je u suštini tehnika izmene (a ne sakrivanja) informacija pomoću neke transformacije, na takav način da samo određena grupa korisnika može izvući originalnu informaciju, a svi drugi ne mogu. Transformacija *otvorenog teksta* informacije u nečitljiv *šifrat*, vrši se upotrebom kriptografskog algoritma i kriptografskog ključa. Kriptografija se deli na: *simetričnu, asimetričnu (PKI), hash funkcije i naprednu kriptoanalizu*. Za izvlačenje otvorenog teksta iz šifrata, u slučaju *simetrične kriptografije,* ovlašćeni korisnici imaju isti ključ, a kod *asimetrične kriptografije* ili infrastrukture sa *javnim* ključem – PKI, imaju matematički par *javnog i privatnog* ključa. U savremenim kriptografskim sistemima bezbednost informacija je više u ključu nego algoritmu, jer je praktično nemoguće čuvati u tajnosti algoritam u komercijalnom okruženju, dok je čuvanje tajnosti ključa samo problem procesa upravljanja ključem [5]. Vrednovanje kriptografskih algoritama vrši se na osnovu kriterijuma za procenu (Tabela 8.3). Vrednosti simetričnih i asimetričnih algoritama za mehanizme zaštite u odnosu na relevantne kriterijume date su u Tabeli 8.4 [67].

Tabela 8.3. Kriterijumi procene vrednosti kriptološkog algoritma

Vrednost (poeni)	Prihvatljivost metode za mehanizam zaštite
5	Veoma prihvatljiv
4	Prihvatljiv
3	Prosečan (bez posebnih prednosti)
2	Relativno loš
1	Vrlo loš
0	Bez opredelenja

Tabela 8.4. Vrednovanje kriptoloških algoritama za mehanizme zaštite

Kriterijum	Asimetrični algoritam	Simetrični algoritam
Identifikacija	5	3
Autentifikacija	5	5
Podaci	3	3
Kašnjenje	4	2
Troškovi	1	5
Kvalitet prenosa	0	0
Opterećenje kanala	1	5
Ukupno	19	23

Simetrični algoritmi su bolji metod kriptozaštite, uzimajući u obzir sve kriterijume, iako su asimetrični algoritmi u prednosti u odnosu na nivo zaštite. Asimetrični algoritmi su bolji za autentifikaciju korisnika, jer se mogu kombinovati sa uređajima za jaku autentifikaciju (smart kartice, tokeni), dok su ekvivalentni simetričnim algoritmima za zaštitu sadržaja informacija i podataka, jer koriste odgovarajući stepen kriptozaštite, bez obzira na tip algoritma.

Kriptografski mehanizmi koriste se u arhitekturi zaštite RS za šifrovanje celog čvrstog diska (npr. Windows VISTA, Windows 7), baza podataka ili datoteka (npr. Win XP OS), a u RM za zaštitu poverljivosti podataka na prenosnom putu i za implementaciju integrisanih servisa zaštite – *autentifikacije, poverljivosti, integriteta i neporecivosti informacija* u PKI sistemu. Za zaštitu integriteta podataka kriptografski algoritam od originalnih podataka pravi sažetak (*hash*) ili *digitalni potpis*, koji se zatim šifruju i skladište na bezbednom mestu. Ako neovlašćeni korisnik izmeni podatke, ne može se rekonstruisati originalna *hash* funkcija ili potpis, što vlasnik može dokazati verifikacijom, jer poseduje ključ.

8.3.6.1. Osnovi kriptografije – simetrični šifarski sistemi

Kriptografski mehanizmi i protokoli zaštite imaju najznačajniju primenu za zaštitu informacija na prenosnom putu kroz potencijalno ne-prijateljske mreže. Za zaštitu se koriste specifično dizajnirani protokoli, koji implementiraju i izvršavaju jedan ili više mrežnih servisa zaštite: *autentifikaciju, zaštitu poverljivosti, zaštitu integriteta i neporecivosti*.

Kriptografske transformacije su matematičke funkcije, odnosno, algoritmi sa kojim se nizovi bitova otvorenog teksta (OT) prevode u nizove bitova šifrovanog teksta ili šifrata (ŠT) i obratno. *Šifrovanje* je postupak prevođenja podatka OT u nečitljiv oblik – ŠT, a formalno se može zapisati u sledećem obliku:

$$C = E(P, K_E),$$

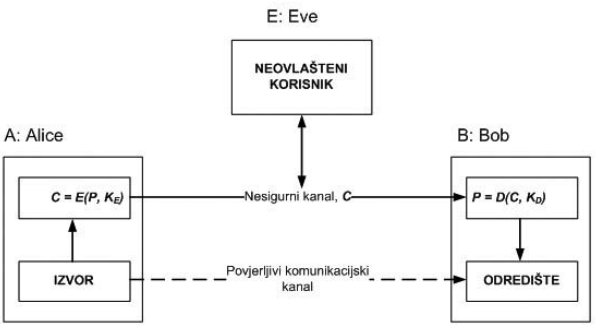
gde su: ***P*** – OT; ***C*** – ŠT; ***E***-funkcija šifrovanja; $\mathbf{K}_E$-ključ za šifrovanje.

Obrnuti postupak prevođenja ŠT u OT naziva se *dešifrovanje*:

$$P=D(C, K_D),$$

gde su: ***P*** – OT; ***C*** – ŠT; ***D*** - funkcija dešifrovanja; $\boldsymbol{K_D}$ - ključ za dešifrovanje.

Funkcije šifrovanja i dešifrovanja zajedno čine *šifarski sistem*. Komunikacioni kanal sa šifrovanjem podataka između dva korisnika prikazan je na Sl. 8.8.



Sl. 8.8. Komunikacija sa šifrovanjem podataka

Alice šalje poruku Bobu, šifrovanu ključem $\boldsymbol{K_E}$, a Bob je dešifruje ključem $\boldsymbol{K_D}$, a Eve je napadač, koji može prisluškivati nezaštićen kanal. Komunikacija između izvora i odredišta predstavlja siguran kanal zahvaljujući šifrovanju poruka.

Osnovna podela šifarskih sistema je na *simetričnu* i *asimetričnu* kriptografiju. Kod simetrične kriptografije ključevi za šifrovanje i dešifrovanje su jednaki: $K_E = K_D$ **= K,** pa je: ***C = E(P, K)***; ***P = D(C, K)***; ***P = D[E(P, K), K]***. Za proces šifrovanja u *simetričnoj kriptografiji* potrebno je znati kriptološki algoritam i tajni ključ. Svi savremeni simetrični algoritmi su javno dostupni pa skrivanje algoritma ne doprinosi bezbednosti. Zbog toga ih je u potpunosti moguće testirati metodima kriptoanalize i proveriti njihovu otpornost na napade. Bezbednost simetričnih algoritama zavisi od snage samog algoritma, ali pre svega od tajnosti i dužine ključa. Najpoznatiji simetrični algoritam je DES (*Data Encryption Standard*) sa K= 56 bita, razvijen u IBM (1977). Ostao je standardni simetrični algoritam sve do 2000. godine, kad ga je zamenio AES (*Advanced Encryption Standard)*, koji koristi ključeve dužine 128, 192 i 256 bita. DES su probili hakeri sredinom 90–tih godina, udružujući procesorsku snagu svojih računara u *virtuelni super računar*. Osnovni nedostatak simetrične kriptografije je upravljanje, odnosno, distribucija ključa. Sigurna razmena ključa je ozbiljan problem, posebno za komunikacije na većim udaljenostima i sa više učesnika. Za ***n*** korisnika u komunikaciji potrebno je ***n(n – 1)/2*** ključeva, čije je generisanje i upravljanje nepraktično, a razmena nesigurna. Ovo je dovelo do pojave asimetrične kriptografije.

Kriptografski ključevi se tretiraju kao resursi IKTS koje treba izuzetno štititi. Čuvanje i upravljanje kriptografskim ključevima uvek se stepenuje najvećim stepenom tajnosti. Funkcija upravljanja ključevima obuhvata sledeće aktivnosti: generisanje, prenos (razmenu), uništavanje, obezbeđenje integriteta i način korišćenja kriptografskih ključeva. Kriptografski ključ se generiše kao slučajni ili pseudoslučajni niz (simetrični) ili kao proizvodi prostih brojeva velikog broja (PKI). Prenos simetričnih ključeva mora biti tajni (sačuvati tajnim sadržaj ključa). Kod prenosa javnih ključeva ne postoji problem razmene, ali ostaju problemi integriteta ključeva, koji se rešavaju u kontekstu zaštitne mrežne arhitekture. Razmena ključeva korisnika u mreži može se vršiti direktno ili indirektno.

8.3.6.2. Osnovi kriptografije – asimetrični šifarski sistemi

Asimetrična kriptografija ili Infrastruktura sa javnim ključem (**PKI**), jedna je od najbitnijih *infrastrukturnih komponenti zaštite* RM iz više razloga [5, 37, 58, 74]:

- obuhvata veći broj korisnika od simetrične kriptografije,
- svaki korisnik zahteva samo par ključeva za komunikaciju sa svim ostalim,
- delimično rešava problem distribucije ključa kod simetrične kriptografije,
- obezbeđuje okvir za protokole zaštite transakcija i
- integriše servise *digitalnog potpisa, zaštite CIA i jake autentifikacije*.

U PKI svaki korisnik u vezi ima jedinstven matematički par javnog (**Pk)** i privatnog ključa (**Tk**). Javni ključ se razmenjuje sa svim korisnicima u mreži, a privatni strogo čuva. Glavni nedostatak PKI sistema je poverenje korisnika u povezanost **Pk** i nominalnog vlasnika. Iako se **Pk** ne mora čuvati u tajnosti kao simetrični, teško je u *on line* režimu rada povezati javni ključ sa njegovim vlasnikom.

Uobičajen način za povezivanje **Pk** sa vlasnikom je pomoću *digitalnog sertifikata* (**DS**) – elektronskog dokumenta, koji povezuje **Pk** sa imenom vlasnika na poverljiv i bezbedan način. **DS** je neka vrsta *digitalnog pasoša*, uspostavlja identitet, neophodan za autentifikaciju korisnika i poruka i pouzdano pridružuje dati par ključeva **(Pk, Tk)** identitetu korisnika. Može se primenjivati za *verifikaciju digitalnog potpisa, kontrolu pristupa web aplikacijama i za proceduru jake autentifikacije.* **DS** mora biti usaglašen i lak za lociranje i autentifikaciju. Može imati standardni format (npr. X.509), a i ne mora. Deli se prema nameni na: *DS identiteta* – kodira identitet principala, *DS atributa* – kodira grupni kredibilitet, *DS ovlašćenja* – kodira delegiranje i restrikcije ovlašćenja, *DS uslova korišćenja* – kodira npr. troškove, atribute uloga, lične karakteristike i sl. Generalno, DS je struktuiran u tri *promenljiva dela* i sadrži **Pk** vlasnika. **Prvi deo** – *tbsCertificate* su podaci značajni za identifikaciju DS*,* **drugi deo** – *signature Algorithm* je identifikator algoritma za potpisivanje*,* a **treći deo** – *Signature* je sam digitalni potpis [37].

Prvi deo uključuje: *Validnost DS* – početak i kraj važnosti DS; *Vlasnika DS* – ime vlasnika DS, kojem se pridružuje Pk, odeljenje i uloga u organizaciji, e-mail, region u državi, oznaka države; *Verzija* (1,2 i 3); *Serijski broj* – jedinstven redni broj izdatog DS; *Ime izdavača DS* (*Issuer*) – identifikuje sertifikaciono telo – **CA** (*Certification Authority*); *Javni ključ* – ***Pk*** vlasnika DS i identifikator algoritma za koji je namenjen (RSA, DSA, ECDSA); *Dodatne informacije* – kritične i nekritične (identifikatore Pk za proveru DS, namenu Pk, uslove kreiranja i korišćenja DS, alternativna imena CA i vlasnika DS). Ako aplikacija koja koristi DS pronađe *CRITICAL* i ne prepozna ga, mora odbaciti DS kao neispravan;

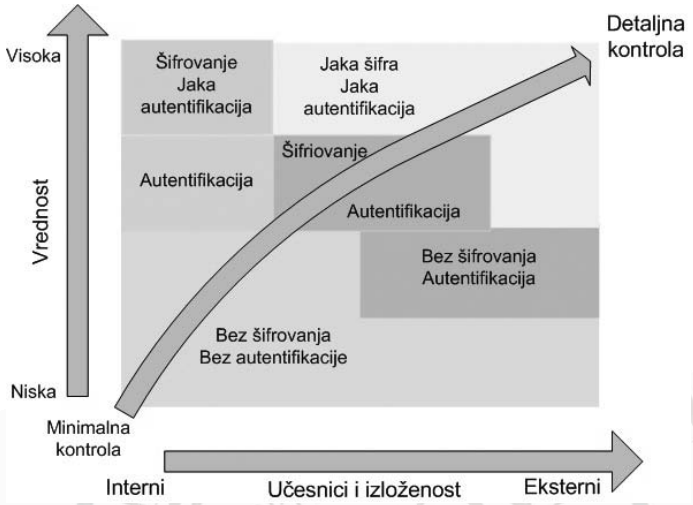
Drugi deo je *identifikator algoritma* za digitalno potpisivanje (RSA, DSA...) i *heš* funkcije (MD5, SHA1, SHA2...) za generisanje digitalnog potpisa CA.

Treći deo je *digitalni potpis* (DP) sa **Tk** CA. DP je analogan ručnom potpisu i osigurava autentičnost. Tipičan proces DP – generisanje heš vrednosti dokumenta/ potpisa i šifrovanje te *heš* vrednosti sa **Tk** autora, što osigurava integritet dokumenta/potpisa. DP ne obezbeđuje zaštitu poverljivosti sadržaja dokumenata. Obično se dodaje čistom tekstu dokumenta i omogućava verifikaciju integriteta sadržaja (Sl. 8.9).

Verzija formata sertifikata
Serijski broj sertifikata
Identifikator algoritma kojim se vrši digitalni potpis
Naziv Sertifikacionog tela koje je izdalo sertifikat
Rok važnosti sertifikata
Naziv vlasnika sertifikata
Javni ključ vlasnika sertifikata
Određeni specifični podaci koji se odnose na uslove korišćenja sertifikata
DIGITALNI POTPIS SERTIFIKATA TAJNIM KLjUČEM SERTIFIKACIONOG TELA

Sl. 8.9. Sadržaj standardnog ITU X.509 DS–3–0

Izbor mehanizama zaštite generalno zavisi od vrednosti imovine, koja se štiti i stepena izloženosti napadima. Na Sl. 8.10. prikazan je zahtevani nivo mehanizama zaštite za aplikacije ili procese, u odnosu na poslovnu vrednost i izloženost [8].



Sl. 8.10. Zavisnost mehanizama zaštite od vrednosti imovine i izloženosti

8.4. REZIME

Za klasifikaciju tehničkih alata za zaštitu koristi se objektno-orijentisana šema, koja obuhvata tri klase alata: *mehanizme zaštite RS (host-orijentisane),* namenjene za poboljšanje podsistema zaštite prirodnog OS – NOSSS hosta (servera ili radne stanice), aplikacija i podataka; *mrežno orijentisane alate* (mehanizme i protokole) za zaštitu RM i *mehanizme za infrastrukturnu podršku* (PKI, smart kartice i autentifikacioni uređaji). Unutar prve dve klase, alati zaštite dalje se klasifikuju na mehanizme za *autentifikaciju i autorizaciju* (RS/RM), *zaštitu integriteta* (RS/RM), *kontrolu pristupa* (RS/RM), *monitoring* (RS/RM) i *zaštitu poverljivosti, integriteta i raspoloživosti podataka i informacija*. U ovoj klasifikaciji važno je razumeti razlike između integriteta RS/RM i informacija.

Model troslojne strukture apstraktnih nivoa u RS koristi se za definisanje slojeva zaštite u RS. *Operativni sistem* (OS) je najznačajniji apstraktni sloj sistemskih programa, zato što učestvuje u svim zadacima koje RS obavlja. *Zaštita OS određuje najviši nivo zaštite celog* IKTS. Osnovni koncept modela je da viši sloj prima neku vrstu servisa od nižeg sloja softvera. Pošto ovi softveri koriste servise koje nudi OS, njihova zaštita je nužno zavisna od zaštite OS i, ako je OS probijen direktno preko sloja aplikacija, lako je zaobići mehanizme zaštite baza podataka i srednjeg sloja. Zato je NOSSS osnovni sloj

zaštite RS, koji treba komplementarno jačati dodavanjem drugih tipova kompatibilnih softvera zaštite.

Generički servis logičke kontrole pristupa uključuje komponente za i *identifikaciju, verifikacije identiteta* ili *autentifikaciju* korisnika sistemu/aplikaciji i za *autorizaciju,* legalnim korisnicima, prava pristupa i aktivnosti na objektima IKTS. Servis kontrole pristupa može se zasnivati na bazi mehanizama *mainframe tipa* – liste kontrole pristupa (ACL), uloga (RBAC), atributa (ABAC), politike zaštite (PBAC) i adaptivnog praćenja rizika (RAdAC). Mehanizmi LAC se još mogu klasifikovati u LAC na osnovu obaveze (MAC) i diskrecionog prava vlasnika (DAC). Savremeni softverski mehanizmi za LAC različitim platformama, tzv. mehanizmi za *administraciju korisnika organizacije* – EUA (*Enterprise User Administration*), rade sa NOSSS na većini platformi i centralizuju upravljanje LAC u distribuiranom okruženju IKTS.

Monitoring zaštite RS vrše sistemi za detekciju i sprečavanje upada u RS – IDPS, koji prepoznaju pokušaje upada, upozoravaju korisnike i vrše korektivne akcije. IDPS sistemi (HIDPS-za RS i NIDPS-za RM) dele se, prema principima detekcije, na sisteme koji koriste tehniku *detekcije na bazi potpisa* i složene detektore *anomalija*. Savremeni koncept IDPS koristi određene vrste inteligentnih zamki za napadača (*hony pot*), kojima skreću njihovu pažnju i izučavaju osobenosti u cilju preventivne zaštite od sledećeg napada.

Mehanizmi za upravljanje log datotekama obezbeđuju selektivan pristup log datotekama kontrolnih tragova bezbednosno relevantnih događaja i smanjuju problem obima podataka, filtriranjem na osnovu implementiranog skupa pravila. Cilj je standardizacija reprezentacije kontrolnih tragova, tako da administratori mogu analizirati, a ne samo interpretirati podatke.

Integritet RS kontrolišu *skeneri ranjivosti (zaštite) sistema*, koji se obično dele na *skenere ranjivosti (zaštite) RS* i *skenere ranjivosti (zaštite) RM*. Skeneri zaštite RS rade na principu periodičnog monitorisanja aktuelne konfiguracije i njenim poređenjem sa predefinisanom. *Skeneri sadržaja i filteri e–pošte* mogu analizirati sadržaj preuzetih mobilnih kodova ili poruka e–pošte radi detekcije potencijalne povrede sistema zaštite i izvršavanje akcije odgovora na pretnje; mogu detektovati steganografski ugrađene slike i tekst u poruke e-pošte i smestiti ih u karantin za dalju analizu. U ovom slučaju skeneri sadržaja direktno se koriste za zaštitu samih podataka. Skeneri sadržaja su komplementarni sa AVP – analiziraju sadržaje poruka i evaluiraju ih u odnosu na predefinisanu politiku, a zatim izvršavaju neke akcije, kada sadržaj ne ispunjava zahteve politika zaštite. Računarski virusi i drugi maliciozni programi narušavaju integritet RS. AVP ispituje otkriveni maliciozni program i ako identifikuje *potpis* malicioznog programa aktivira set instrukcija za uklanjanje.

Za servis zaštite poverljivosti koriste se simetrični i asimetrični kriptografski mehanizmi – tehnike izmene informacija pomoću neke transformacije, na takav način da je samo određena grupa korisnika može izvući u originalnom tekstu. Kriptografski mehanizmi koriste se u arhitekturi mrežne zaštite za implementaciju integrisanih servisa zaštite – *autentifikacije, poverljivosti, integriteta i neporecivosti* informacija.

8.5. KLJUČNI TERMINI

Alati zaštite: hardversko–softverski mehanizmi i protokoli zaštite (tehničke kontrole zaštite); u širem smislu uključuju proceduralne kontrole zaštite.

Antivirusni programi: programi koji sadrže potpise poznatih malicioznih kôdova, sa kojim porede tekuće, detektovane kôdove, uklanjaju ih ili stavljaju u karantin.

Autentifikacija: proces sa kojim korisnik (lice ili program) dokazuje svoj identitet sistemu ili aplikaciji koji nude neki servis; verifikacija identiteta.

Autorizacija: proces dodeljivanja legalnom korisnicima prava pristupa objektima IKTS.

Autorizacioni serveri: pridružuju skup prava pristupa autentifikovanim entitetima.

Host–orijentisani alati: mehanizmi zaštite namenjeni za poboljšanje zaštite NOSSS hosta (servera, radne stanice), aplikacija i podataka.

Kriptografski mehanizam: tehnika izmene informacija pomoću neke transformacije na takav način da je samo određena grupa korisnika može izvući u originalnom tekstu.

Mehanizmi zaštite: pojedinačni, individualni algoritmi ili metodi ili hardversko–softverski moduli za eliminisanje bezbednosnih problema u mreži.

Podsistem zaštite prirodnog OS: NOSSS (*Native Operation System Security Subsystem)* osnovni sloj zaštite OS u RS; uključuje osnovne mehanizme zaštite za *kontrolu pristupa*, *autentifikaciju korisnika, logovanje bezbednosnih događaja, AVP, šifrovanje fajla i dr*.

Program za administraciju korisnika organizacije – EUA (*Enterprise User Administration*): univerzalno rešenje AC za složene sisteme, različite platforme i interaktivni rad sa postojećim NOSSS na većini platformi; centralizuje upravljanje kontrolom pristupa.

Sistemi za detekciju i sprečavanje upada u sistem – **IDPS:** detektuju pokušaja upada, upozorenje korisnika i korektivne akcije na bazi tehnika detekcije potpisa i anomalija; dele se na HIDPS (za RS) i NIDPS (za RM).

Skeneri sadržaja i filteri e-pošte: analiziraju sadržaj preuzetih mobilnih kodova ili poruka e–pošte, na potencijalne povrede sistema zaštite i reaguju na pretnje.

Skeneri ranjivosti (zaštite) RS: rade na principu periodičnog monitorisanja aktuelne konfiguracije RS i poređenjem ove konfiguracije sa predefinisanom.

***Web* filteri**: mehanizmi mrežne zaštite za AC internih korisnika *web* lokacijama i selektivno blokiranje pristupa zabranjenim *web* lokacijama, na bazi lokalne politike zaštite.

8.6. PITANJA ZA PONAVLJANJE

1. Dobra klasifikacija tehničkih alata je na bazi:
   a. modela životnog ciklusa
   b. klasifikacione *objektno–orijentisane* šeme za softvere zaštite IKTS
   c. strukturnog objektnog pristupa
2. Alati se, u odnosu na tipove *servisa zaštite* koje podržavaju, dele na alate za:
   a. identifikaciju, autentifikaciju i autorizaciju (RS/RM)
   b. fizičku zaštitu (RS/RM)
   c. kontrolu pristupa (RS/RM)
   d. skeniranje sistema zaštite (RS/RM)
   e. zaštitu poverljivosti, integriteta i raspoloživosti podataka i informacija
3. Koncept slojevite zaštite zasniva se na modelu:
   a. slojevite strukture apstraktnih nivoa računarskog sistema
   b. hijerarhijske strukture računarske mreže
   c. životnog ciklusa sistema
   d. vodopada

4. U servisu RBAC autorizacije prava pristupa objektima IKTS:
   a. korisnik može biti član samo jedne grupe
   b. efektivne dozvole korisnika mogu se naslediti samo iz jedne grupe
   c. pravljenjem grupa, administratori prave manje korisničkih naloga
   d. grupe ne mogu imati privilegije, koje se sukobljavaju
5. Centralizovano upravljanje smanjuje posao mrežnom administratoru:
   a. smanjivanjem broja resursa za koje treba korisnicima dati privilegije
   b. smanjivanjem broja grupa koje je potrebno napraviti
   c. smanjivanjem broja korisničkih naloga koje treba napraviti
   d. smanjivanjem broja privilegija koje treba dati svakom korisniku
   e. dodeljivanjem korisniku najmanje prava pristupa
6. Proveru identiteta (autentifikaciju) pomoću tokena najbolje opisuje:
   a. nešto što korisnik jeste
   b. nešto što korisnik ima
   c. nešto što korisnik zna
7. Proveru identiteta (autentifikaciju) pomoću lozinke najbolje opisuje:
   a. nešto što korisnik ima
   b. nešto što korisnik zna
   c. nešto što korisnik jeste
8. Proveru identiteta (autentifikaciju) pomoću biometrike najbolje opisuje:
   a. nešto što korisnik ima
   b. nešto što korisnik zna
   c. nešto što korisnik jeste
9. Privilegovani menadžerski nalog se koristi da obezbedi:
   a. zaštitu OS
   b. rad sa programima za podršku ili sa slojem aplikacija
   c. kontrolu sistema zaštite
   d. kontrolu korisničkih naloga
10. U savremenim kriptografskim sistemima bezbednost je više u:
   a. ključu i procesu upravljanja kriptografskim ključem
   b. algoritmu jer je praktično moguće čuvati u tajnosti algoritam u komercijalnom okruženju
   c. protokolima zaštite
11. Generički servis logičke kontrole pristupa (LAC) uključuje mehanizme za:
   a. identifikaciju, verifikaciju, autentifikaciju i autorizaciju
   b. identifikaciju, autentifikaciju i autorizaciju
   c. identifikaciju, autorizaciju, verifikaciju i autentifikaciju
   d. identifikaciju, verifikaciju i autentifikaciju
12. Diskreciona kontrola (DAC) pristupa se zasniva na:
   a. utvrđenim pravilima
   b. odluci vlasnika sistema
   c. politici zaštite
   d. proceni rizika
13. Obavezna kontrola pristupa (MAC) se zasniva na:
   a. odluci vlasnika sistema
   b. utvrđenim pravilima
   c. listi kontrole pristupa (ACL)
   d. ulogama u organizaciji
14. Kontrola na bazi politike zaštite (PBAC) zasniva se na:
   a. listi kontrole pristupa (ACL)
   b. ulogama u organizaciji
   c. politici zaštite
   d. proceni rizika
15. Univerzalni EUA mehanizmi za centralizovanu AC:
   a. upravlja sa LAC u distribuiranom okruženju
   b. uključuje hardverski modul, upravljačkog agenta i korisnički interfejs
   c. uključuje softverskog agenta, upravljačku aplikaciju i korisnički interfejs
16. Definicija ranjivosti IKTS uključuje:
   a. greške plana zaštite, greške hardvera, greške konfiguracije RS/RM

b. greške softvera, greške hardvera, greške topologije RM
c. greške softvera, greške hardvera, greške konfiguracije RS/RM

17. Proces upravljanja ranjivostima sadrži sledeće faze:
    a. identifikaciju, procenu, remedijaciju, izveštavanje, poboljšanje i monitoring
    b. identifikaciju, planiranje, remedijaciju, izveštavanje i monitoring
    c. identifikaciju, procenu, remedijaciju, poboljšanje i monitoring
18. Za zaštitu integriteta RS koriste se sledeći mehanizmi zaštite:
    a. kriptografski hardversko softverski mehanizmi, skeneri i IDPS
    b. skeneri ranjivosti RS, AVP, skeneri sadržaja, filteri e–pošte, IDPS
    c. skeneri ranjivosti RS, AVP, skeneri sadržaja, filteri e–pošte, IDPS, kriptografski mehanizmi
19. Kriptografija se deli na:
    a. simetričnu, asimetričnu, heš funkcije i naprednu kriptoanalizu
    b. simetričnu, PKI, heš funkcije i naprednu kriptoanalizu
    c. PKI, asimetričnu, kriptozaštitu i kriptoanalizu
20. Simetrična kriptografija je bolji metod zaštite od asimetrične za:
    a. zaštitu tajnosti informacija na komunikacionim linijama
    b. integraciju mehanizama autentifikacije, poverljivosti, integriteta i neporecivosti informacija
    c. antivirusnu zaštitu i digitalni potpis
    d. distribuciju kriptoloških ključeva
21. Asimetrična kriptografija je bolji metod zaštite od asimetrične za:
    a. zaštitu tajnosti informacija na komunikacionim linijama
    b. integraciju mehanizama autentifikacije, poverljivosti, integriteta i neporecivosti informacija
    c. antivirusnu zaštitu i digitalni potpis
    d. distribuciju kriptoloških ključeva
22. Asimetrični kriptološki sistem:
    a. ima samo jedan ključ za šifrovanje i dešifrovanje
    b. ima algoritam i matematički povezan par ključeva – javni i tajni
    c. sadrži glavne module – CA, RA i direktorijum
    d. uključuje kriptološki algoritam, jedinstven ključ i upravljanje ključem
23. Simetrični kriptološki sistem:
    a. ima samo jedan ključ za šifrovanje i dešifrovanje
    b. ima algoritam i matematički povezan par ključeva – javni i tajni
    c. sadrži glavne module – CA, RA i direktorijum
    d. uključuje kriptološki algoritam, jedinstven ključ i upravljanje ključem
24. Glavni nedostatak simetričnog kriptološkog sistema je:
    a. obuhvata manji broj korisnika
    b. svaki korisnik zahteva samo par ključeva za komunikaciju sa ostalim
    c. distribucija ključa
    d. integriše veći broj mehanizama zaštite
    e. ne integriše više mehanizama zaštite informacija
25. Glavne prednosti asimetričnog kriptološkog sistema su:
    a. obuhvata manji broj korisnika
    b. svaki korisnik zahteva samo par ključeva za komunikaciju sa ostalim
    c. distribucija ključa
    d. integriše veći broj mehanizama zaštite
    e. ne integriše mehanizme zaštite

9. TEHNOLOGIJE ZA ZAŠTITU RAČUNARSKIH MREŽA

Po završetku ovog poglavlja razumećete:

- Osnovne razlike i sličnosti tehnologija zaštite RS i RM
- Osnovne alate (mehanizme i protokole) za zaštitu RM
- Infrastrukturne komponente zaštite RM (PKI, smart kartice)
- Standarde, ograničenja i tehnologije zaštite RM (PKI, smart kartice)

9.1. UVOD

Mrežna infrastruktura obuhvata komunikacionu mrežu, uređaje za povezivanje, matične računare i tačke povezivanja sa mrežom. Uspešan napad na mrežnu infrastrukturu može onesposobiti RM ili je izložiti raznim zloupotrebama. Za efektivnu zaštitu mrežne infrastrukture i RM treba poznavati tipove potencijalnih napada. Od većine potencijalnih napada na RM osnovna zaštita je kontrola pristupa kritičnim resursima, protokolima i pristupnim tačkama, uključujući fizičku zaštitu i zaštitu konfiguracija uređaja, neprekidni nadzor mrežnog saobraćaja, zaštitu servera, mobilnih uređaja, radnih stanica i uređaja za umrežavanje, NIDPS, zaštitu udaljenog pristupa (RADIUS, TACAS protokoli) i zaštitu bežičnih RM. Najbitnija komponenta zaštite RM je PKI, koja obezbeđuje brojne prednosti u odnosu na simetrične sisteme, uključujući uređaje za zaštitu kriptografskih tajni *autentifikacioni i autorizacioni serveri, kripto-moduli, smart kartice, tokeni itd.*

Svi tipovi bežičnih mreža inherentno su nebezbedni, jer koriste radio frekvencije za prenos informacija. Bežična lokalna mreža (WLAN), klasičan *Ethernet* LAN bez kablovske infrastrukture, ima najveću praktičnu primenu. WEP protokol (*Wireless Equivalent Protocol*) za zaštitu WLAN, dizajniran da zaštiti *CIA* informacija kao i kod fizičkog LAN-a**,** pokazao je brojne slabosti. *Treća generacija (3–G)* tehnologije bežičnih sistema koriguje uočene bezbednosne ranjivosti WEP.

9.2. SERVIS LOGIČKE KONTROLE PRISTUPA RAČUNARSKOJ MREŽI

9.2.1. Mehanizmi logičke kontrole pristupa računarskoj mreži

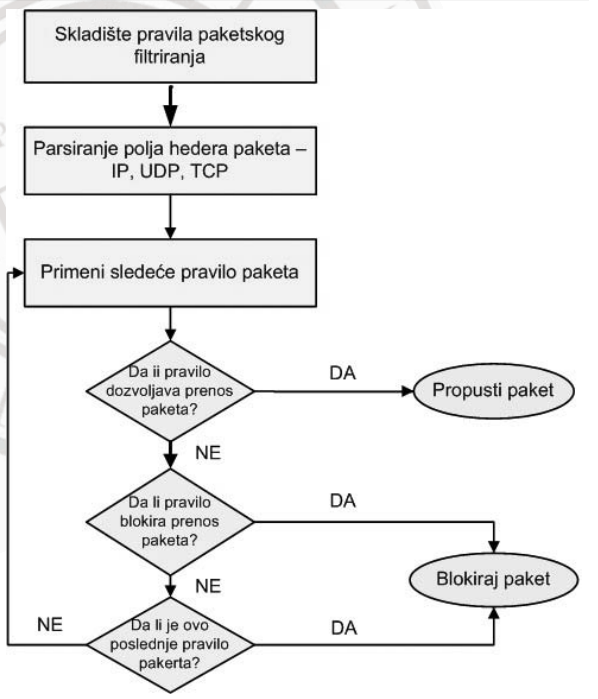
Koncept LAC, kako se primenjuje u RS, u toj formi ne postoji u RM. Za LAC između dve RM mogu se koristiti tehnike kao što su *barijere za filtriranje paketa* u TCP/IP okruženju i *uspostavljanje zatvorenih grupa korisnika* (DMZ), ali ni jedna od ove dve tehnike ne može se koristiti za zaštitu podataka koji putuju fizičkim vezama.

9.2.1.1. Logičke mrežne barijere

Logičke mrežne barijere (*Firewalls*) su uređaji ili konstrukcije uređaja koje nameću politiku LAC između dve RM ili segmenata RM. Barijere *blokiraju* konekcije na bazi politike i rade na nivoima 3 – 7 OSI modela. U TCP/IP modelu slojevi 5, 6 i 7 su deo aplikacija, tako da se politika barijere za blokiranje/dopuštanje pristupa bazira na *mrežnom*, *transportnom* i *aplikativnom* sloju. Barijere generalno kontrolišu saobraćaj na mrežnom nivou, ne prepoznaju protokole koji nisu TCP/IP, pa moraju biti specifično konfigurisane da prepoznaju druge tipove protokola. Očigledno, barijere imaju vrlo ograničeni skup podataka sa kojima mogu raditi, što ograničava i njihove realne rezultate [19].

Većina savremenih rešenja uključuje *autentifikaciju* korisnika, što je glavni napredak u razvoju barijera, pošto omogućava da se mrežna konekcija povezuje sa entitetom (korisnikom, procesom), a ne sa mrežnom adresom (IP). Postoje dve glavne klase komercijalnih, programskih rešenja barijera, koje rade na različitim principima, ali postižu slične rezultate.

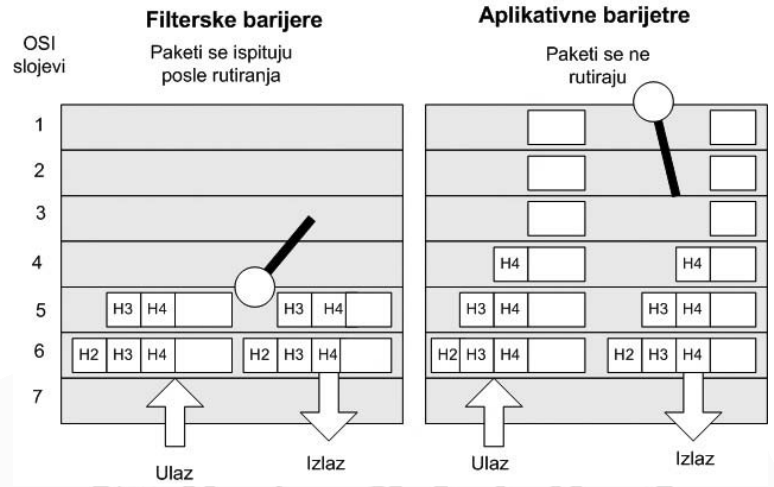
Barijere sa uspostavljanjem veze, kontrolom stanja veze i tehnikom filtriranja rutiranih IP paketa od jednog mrežnog interfejsa do drugog, presreću već rutirane pakete na mrežnom sloju i analiziraju informacije o protokolu od slojeva 3 – 7. Takođe, analiziraju informacije o *stanju* veze, da bi odredile da li pakete treba *blokirati* ili *propustiti*. Za protokole bez uspostavljanja veze (npr. UDP), koristi se virtuelna sesija, u kojoj barijera skladišti informaciju o stanju veze, čak, iako je sam protokol bez te informacije (Sl. 9.1).



Sl. 9.1. Tok procesa filtriranja paketa

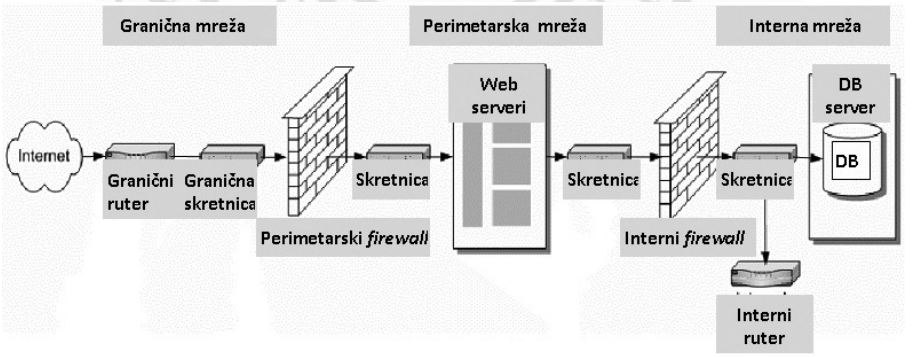
Barijere na aplikativnom sloju poznate kao aplikativna mrežna kapija (*gateway*), ili *proksi,* ne rutiraju direktno pakete. Dolazne pakete procesiraju komunikacioni programi i prenose ih aplikaciji, koja može da čita određeni protokol na visokom nivou apstrakcije. Pošto nameću kontrole na aplikativnom sloju, *proksi* barijere su specifične za aplikacije, što znači da svaki put kada se razvija novi protokol za neku aplikaciju, zahteva se novi *proksi* za zaštitu. U stvarnosti, većina savremenih

protokola nemaju *proksi* barijere, koje ih prate, a *proksi serveri* se uglavnom koriste za kontrolu standardnih Internet protokola, kao što su FTP ili HTTP. Načini rada filterskih i aplikativnih – *gateway* barijera prikazani su na Sl. 9.2. Sve češće proizvođači kombinuju karakteristike obe barijere.



Sl. 9.2. Principi rada filterskih i aplikativnih barijera [19]

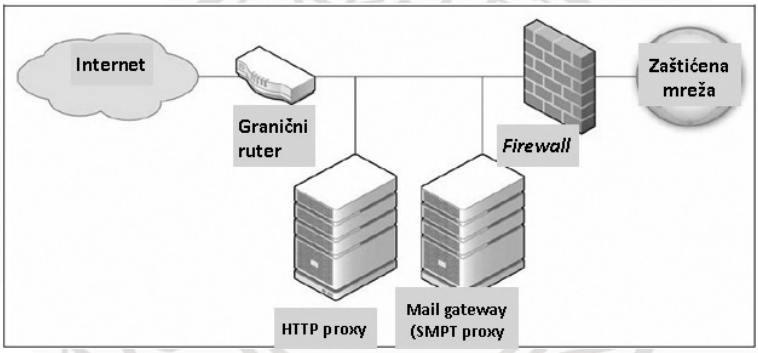
Primer upotrebe barijere za zaštitu perimetra (DMZ) RM prikazan je na Sl. 9.3.



Sl. 9.3. Zaštita perimetra računarske mreže sa dve barijere

9.2.1.2. Proksi serveri

Proksi serveri funkcionišu slično aplikativnim *gateway* barijerama. Dok su barijere namenjene za kontrolu mrežnog pristupa dolaznog i odlaznog saobraćaja, *proksi* serveri su usmereni na kontrolu konekcija koje dolaze iz interne RM. Proksi serveri zahtevaju autentifikaciju krajnjeg korisnika, vrše restrikciju komunikacija na definisani skup protokola, primenjuju restrikciju kontrola pristupa i loguju kontrolne tragove. Najčešći tip proksi servera u praksi su *web proksi serveri*, koji se ne koriste samo za zaštitu. Na primer, jedna od najvažnijih funkcija *web* proksi servera je skladištenje u keš memoriju podataka za poboljšanje performansi. Striktno govoreći, proksi serveri nisu mehanizmi za zaštitu RM i korektnije ih je smatrati višefunkcionalnim mrežnim uređajima, koji implementiraju važnu bezbednosnu funkcionalnost. Na Sl. 9.4. prikazana je konfiguracija servera na aplikativnom nivou.



Sl. 9.4. Konfiguracija aplikativnog proksija [19]

9.2.1.3. Web filteri

Web filteri se koriste za kontrolu pristupa internih korisnika *web* lokacijama, omogućavajući administratoru da selektivno blokira pristup određenim tipovima *web* lokacija, na bazi lokalne politike zaštite. Koriste se i za kontrolu produktivnosti zaposlenih i sprečavanje pristupa zabranjenim *web* lokacijama.

Odluka o blokiranju/dopuštanju pristupa, *web* filter donosi na bazi konsultovanja instalirane baze podataka o potencijalno problematičnim *web* lokacijama, koje održavaju i regularno ažuriraju proizvođači, slično ažuriranju AVP. Neki proizvodi poseduju inteligentne agente, koji analiziraju sve posećivane *web* lokacije i ažuriraju baze podataka. Ovi mehanizmi tipično uključuju *mogućnost blokiranja određenih kategorija sadržaja sa web lokacija, restrikcije za određeni period dana, definisanje načina monitorisanja pokušaja pristupa, izdavanje standardnih i kastomizovanih izveštaja i praćenje ponašanja korisnika i poseta lokacijama*.

9.2.1.4. Autentifikacioni protokoli

Glavni bezbednosni problem postojećih TCP/IP mreža je lakoća, sa kojom se podaci mogu presresti i analizirati. Zato, svaki mehanizam autentifikacije koji se oslanja na lozinke u otvorenom tekstu (OT) ili bilo koja predvidljiva razmena podataka, nije bezbedna u mrežnom okruženju. Standardni mrežni protokoli obezbeđuju dobru funkcionalnost, ali pokazuju i određene ranjivosti (Tabela 9.1). Zaštita mrežne infrastrukture deo je rešenja ovog problema, ali ne obuhvata mogućnost da neovlašćeni korisnik može koristiti svoju opremu za pristup mreži i aktivirati *snifer* (skener prisluškivač) ili sličan alat za kontrolu saobraćaja u RM. Takođe, ne možemo, u WLAN mrežama ili na Internetu, verovati u mehanizme zaštite drugih korisnika. Zato je neophodno ugraditi mehanizme zaštite u sam proces razmene podataka. Uobičajen način, da se ovo uradi, je korišćenje standardnih *autentifikacionih protokola* [35, 36, 74].

Tabela 9.1. Mrežni protokoli sa poznatim ranjivostima

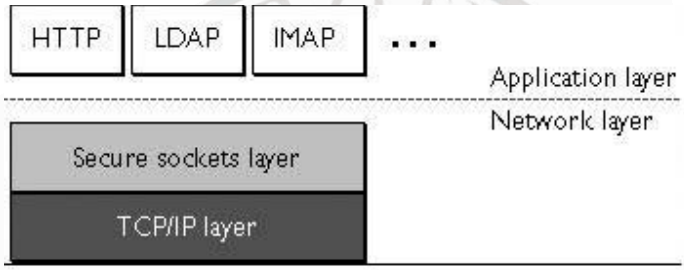
Protokol	**Osnovne ranjivosti**
FTP	Nema kriptozaštitu, izlaže korisničko ime, lozinke i podatke u OT.
TELNET	Ranjiv na preplavljivanje bafera, povratni odgovor i *spoofing* za dobijanje privilegija i otkrivanje lozinke.
HTTP	Više ranjivosti u raznim implementacijama; slaba konfiguracija HTTP servera omogućava eskalaciju privilegija.
LDAP i MS *Directory Services*	Neke implementacije su podložne preplavljivanju bafera i DoS napadima sa mogućnošću izmene privilegija.
SNMP	Mogući DoS napadi i preplavljivanje bafera, ako ostane ime organizacije i dr. podaci u predefinisanoj konfiguraciji; može omogućiti eskalaciju privilegija i kompromitaciju.
SSH (*Secure Shell*)	Kada protokol radi pod nalogom ruta, mogući su DoS napadi, eskalacija privilegija i kompromitacija.
DNS	Više bezbednosnih ranjivosti u raznim implementacijama.

Autentifikacioni protokoli su posebna oblast. Primer autentifikacionih protokola je *NeedhamSchroeder* protokol, upotrebljen u *Kerberos* sistemu u *Windows NT 4.0* i kasnijim *OS*, koji ima ranjivost – omogućava napadaču pristup, upotrebom starog ključa. Autentifikacioni uređaji (*smart kartica, biometrijski uređaj, token)* obezbeđuju korisniku neki fizički identifikator, koji se zahteva za kompletiranje autentifikacije.

Autentifikacioni protokoli se, uglavnom, zasnivaju na konceptu *upita – odgovora* ili razmene *digitalnih sertifikata*. Osnovna ideja je da sistem zahteva dokaz o identitetu, a korisnici inicijalno koriste neki drugi mehanizam za razmenu kriptografskih ključeva. Kada korisnik zahteva pristup, identifikuje se sistemu, koji odgovara sa slučajnim upitom

(*chalange*). Korisnik šifruje ovaj upit, koristeći svoj tajni ključ i šalje nazad sistemu, koji koristi matematički par istog ključa (javni ključ korisnika) za dešifrovanje originalne informacije. Ako je korisnik jedina osoba, koja poseduje tajni ključ, neophodan za šifrovanje slučajnog upita sistema, ovo je verifikacija identiteta. Ako upit nije slučajna vrednost, zlonamerni korisnik ga može presresti, lažno se predstaviti i izdati novu vrednost upita korisniku, primiti transformisani odgovor i obezbediti pristup ciljnom sistemu.

Treba uočiti da autentifikacija nije isto što i uspostavljanje bezbedne sesije i da svaka konekcija, koja ne koristi dodatne mere zaštite, kao što su mehanizmi za šifrovanje ili zaštitu integriteta, može biti kompromitovana. U jednostavnom slučaju, autentifikacija korisnika uključuje unošenje lozinke preko uspostavljene bezbedne sesije, kao što je **SSL** (*Secure Socket Layer*) protokol. Položaj SSL protokola u višeslojnoj arhitekturi RM prikazan je na Sl. 9.5



Sl. 9.5. Lokacija SSL protokola u višeslojnoj arhitekturi RM

Ovaj metod autentifikacije korisnika često se koristi za pristup *web* aplikacijama na Internetu. SSL je osnovni protokol za zaštićen prenos lozinke. SSL protokol obezbeđuje autentifikaciju servera klijentu, klijenta serveru i uspostavu bezbedne, kriptološki zaštićene, komunikacije između klijenta i servera. Osnovni element za dokazivanje autentičnosti kod SSL protokola je *digitalni sertifikat,* koji izdaje sertifikaciono telo – CA (*Certification Authority*). Digitalni sertifikati, između ostalog, sadrže javne ključeve entiteta, koji ih razmenjuju. Programska podrška za upravljanje SSL protokolom na računaru klijenta/servera proverava valjanost digitalnog sertifikata datog servera/klijenta. Svi podaci koji se razmenjuju između klijenta i servera se šifruju na računaru pošiljaoca, a dešifruju na računaru primaoca, čime se vrši zaštita poverljivosti sesije. Podaci se pre slanja digitalno potpisuju i na taj način se postiže zaštita integriteta podataka sesije [5].

SSL protokol koristi dva podprotokola: (1) **SSL protokol zapisa poruka** (*SSL record protocol*), koji definiše formate poruka za prenos podataka i (2) **SSL protokol dogovaranja parametara sesije** (*SSL handshake protocol*), koji se koristi za razmenu poruka, sastavljenih prema SSL protokolu zapisa poruka, između SSL klijenta i SSL servera kada se među njima po prvi put uspostavlja SSL veza.

SSL protokol podržava više različitih kriptografskih algoritama za međusobne autentifikacije klijenta i servera, razmene digitalnih sertifikata i uspostavu tajnih simetričnih ključeva (tj. ključeva sesije). Kriptografski algoritmi korišćeni kod komunikacije SSL protokolom prikazani su u Tabeli 9.2.

Tabela 9.2. Kriptografski algoritmi za komunikaciju SSL protokolom

Algoritam	Opis i primena kriptografskog algoritma
DES	*Data Encryption Standard* – standardni algoritam za šifrovanje podataka
DSA	*Digital Signature Algorithm*
KEA	*Key Echange Algorithm* za razmenu simetričnih ključeva
MD5	*Message Digest* v. 5, *hash* funkcija i algoritam za digitalno potpisivanje
RC2 i RC4	*Rivest Ciphers* simetrični kriptografski algoritmi koje je razvio *Ron Riverst*
RSA	Asimetrični algoritam za šifrovanje i autentifikaciju
RSA key exchange	Algoritam za razmenu simetričnih ključeva kod SSL protokola zasnovan na RSA algoritmu
SHA–512	*Secure Hash Algorithm*, *hash* funkcija dužine 512 bita
Triple–DES	*DES* algoritam primenjen tri puta nad istim podacima

Algoritmi za razmenu ključeva, *KEA* i *RSA key exchange*, određuju način na koji klijent i server dogovaraju simetrični ključ, koji će koristiti u SSL sesiji. U najvećem broju slučajeva koristi se *RSA key exchange* algoritam. Tokom uspostavljanja SSL sesije, odnosno u fazi dogovaranja kriptografskih parametara, klijent i server biraju najjači skup kriptografskih algoritama, koji oba istovremeno podržavaju i koriste tokom SSL sesije. SSL sesija između klijenta i servera uvek započinje razmenom poruka SSL protokola dogovaranja parametara sesije, koji omogućava korisniku da izvrši autentifikaciju servera, primenom PKI metoda, a klijentu i serveru da zajedno učestvuju u generisanju i izboru simetričnog tajnog ključa sesije, koji se koristi za šifrovanje, dešifrovanje i digitalno potpisivanje poruka tokom SSL sesije. Ako server to zahteva, SSL protokol dogovara parametre sesije i omogućava da i server izvrši autentifikaciju klijenta.

Autentifikacioni SSL protokoli dopuštaju napad ubacivanjem čoveka u sredinu i uticaj na većinu servera na Internetu. Ranjivost omogućava da se napadač ubaci u SSL protokol na komunikacionom putu. Pri tome ni veb server ni veb pretraživač ne mogu otkriti da je sesija oteta. Ranjivost dolazi u standardu protokola (formalno poznat kao TLS – Transport Layer Security). Većina SSL implementacija je ranjiva na neki način. Scenario napada uključuje korisnika koji plaća online *račune, banku koja koristi protokole zasnovane na veb servisima i druge aplikacije kao što su mail serveri, serveri baza podataka itd. Sve biblioteke SSL treba bezbednosno popraviti*[28].

28 *The Help Net Security News*, 05.11.2009.

9.2.1.5. Serveri za autentifikaciju i autorizaciju

Autentifikacioni i a*utorizacioni (A&A) serveri* obezbeđuju centralizaciju upravljanja procesom *autentifikacije* – verifikacije identiteta i *autorizacije* – pridruživanja skup privilegija autentifikovanim entitetima. Iako *A&A* serveri nisu obavezni u sistemima za kontrolu udaljenog pristupa, uobičajeno se koriste za ovaj servis. Na primer, u *Windows* OS primarni kontroler domena (PDC) efektivno radi kao autentifikacioni server za *Windows* klijente u lokalnoj mreži.

Serveri za *A&A* obezbeđuju odgovarajuće servise za više klijenata u klijent-server arhitekturi. Mogu obezbediti zaštitu za sve apstraktne slojeve sistema, sve dok su klijenti opremljeni sa odgovarajućim interfejsom i korektno konfigurisani. Neki serveri mogu dodeljivati uloge korisnicima (npr. *CISCO A&A* serveri) [23]. Tipičan primer kako *A&A* serveri rade, uključuje udaljenog korisnika, koji bira broj servera organizacije preko javne telefonske (PSTN) mreže. Uređaj poznat kao *server mrežnog pristupa* – **NAS** (*Network Access Server*) prima vezu od PSTN i nakon autentifikacije korisnika i primene neke restrikcije, dopušta konekciju na zahtevani interni host. Za ove funkcije NAS može koristiti lokalnu bazu podataka ili, što je češće – servise A&A servera. U serverskoj konfiguraciji NAS je posrednik između korisnika i servera, prenoseći svaki zahtev za informacijama od servera prema klijentu i vraćajući odgovor serveru. Kada server ima dovoljno informacija da prihvati/odbije zahtev klijenta, tada šalje odgovor NAS-u, koji izvršava odluku prihvatanjem/odbijanjem konekcije prema predefinisanoj politici. Metod autentifikacije i upravljanje pravima pristupa kontroliše lokalna organizacija, koja može koristiti razne tehnologije, kao što su lozinke, tokeni ili smart kartice.

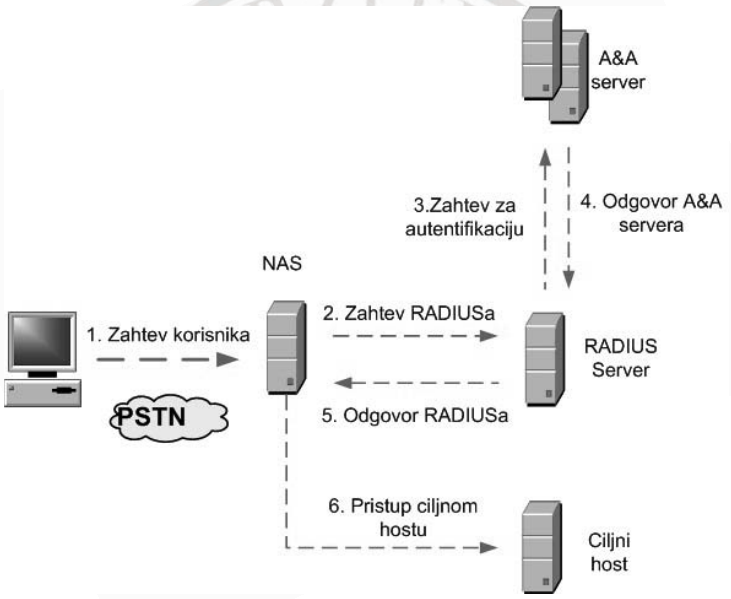
Fleksibilnost podrške različitih metoda A&A postiže se implementacijom standardnog protokola na nivou aplikacija između NAS i bezbednosnog servera. Ovi se protokoli dizajnirani da podrže generičku razmenu između NAS i servera koji ne zavisi od procesa A&A. Postoje dva glavna protokola koji se danas koriste – RADIUS (*Remote Authentication Dial In User Service*) protokol i TACACS + (*Terminal Access Controller Access Control Service*) protokol (Tabela 9.3) [80, 9].

Tabela 9.3. Autentifikacioni i autorizacioni protokoli

RADUUS	***TACACS+***
izvršava se preko UDP	Izvršava se preko TCP protokola
sadrži korisnički profil za autentifikaciju sa svim parametrima korisnika	razdvaja autentifikaciju i autorizaciju
koriste ga računari i mrežni uređaji	koriste ga mrežni uređaji (ruteri, svičeri)

Funkcionalni model RADIUS protokola, kojeg koristi neki NAS za udaljeni pristup korisnika ima sledeće sekvence aktivnosti (Sl. 9.6):

- korisnik inicira *dial-up* vezu sa NAS serverom; NAS traži korisničko ime i lozinku, koje korisnik dostavlja NAS-u sa zahtevom;
- NAS radi kao RADIUS klijent i šalje zahtev za pristup RADIUS serveru;
- RADIUS server prenosi autentifikacione podatke na A&A server, što može uključivati i korišćenje sopstvenog (autorskog) protokola;
- server za A&A dopušta/odbija zahtev;
- RADIUS server odgovara NAS–u sa porukom da prihvata/odbija pristup, zavisno od rezultata autentifikacije;
- ako je autentifikacija uspešna, NAS server dopušta pristup ciljnom hostu.



Sl. 9.6. Funkcionalni model RADIUS protokola

Korišćenje servera za A&A značajno povećava bezbednost pristupa udaljenih korisnika, ali stvarni nivo bezbednosti dostiže se u zavisnosti od primenjenog metoda A&A. Tako lozinka ne obezbeđuje visoku bezbednost, dok kriptografski mehanizam *upit – odgovor* tipa predstavlja značajnu barijeru za napadača. Izbor zavisi od procene rizika. Međutim, čak i sa visoko bezbednom implementacijom, tehnike A&A ne štite podatke, koji se izmenjuju između korisnika i internog RS, kada se veza jednom uspostavi. Zato treba ići korak dalje i implementirati zaštitni protokol između krajnjeg korisnika i odgovarajućeg terminala iza NAS. Ovo rešenje štiti poverljivost podataka i integritet same sesije.

Za web aplikacije, sa zahtevom za visoki stepen skalabilnosti, razvijen je EAM (*Extranet Access Management*) programski paket koji obezbeđuje servise A&A u ekstranet okruženju (što je suprotno udaljenom pristupu).

9.2.1.6. Smart kartice i kriptografski moduli

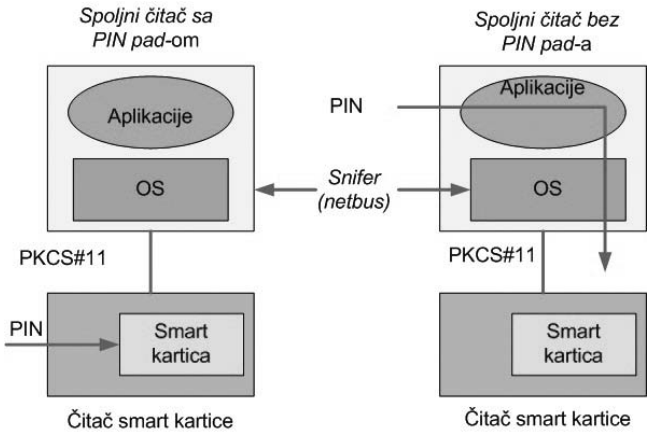
Autentifikacioni uređaji obezbeđuju korisniku neki fizički identifikator, koji se zahteva za uspešan proces autentifikacije. Većina poznatih uređaja za autentifikaciju spada u kategorije *smart kartica* i *biometrijskih uređaja i tokena.*

Za visoku bezbednost RM, u prvom redu, koriste se *smart* kartice i kriptografski moduli za zaštitu kriptografskih tajni. Sa aspekta fizičkih karakteristika, postoje tri glavne klase *smart kartica*: *kontaktne* – zahtevaju fizički kontakt sa čitačem kartica, *beskontaktne* – kapacitivno ili induktivno spregnute sa čitačem kartica i *kombinovane kartice* – obezbeđuju oba načina rada [24].

Iako su objavljene bezbednosne ranjivosti *smart* kartice (napadi *diferencijalnom analizom* i *optičkom indukcijom greške*), *smart* kartice se generalno smatraju bezbednim okruženjem za skladištenje kriptografskih ključeva i drugih poverljivih informacija korisnika. Na raspolaganju je veliki broj uređaja sa *smart* karticama tipa bankarskih kartica. U stvari, *smart* kartična tehnologija u velikoj meri je doprinela razvoju koncepta elektronskog plaćanja.

Smart kartice za skladištenje kriptografskih tajni korisnika, štiti pristup podacima sa zahtevom za unošenje personalnog identifikacionog broja – **PIN** (*Personal Identification Number*) ili nekog biometrijskog parametra (otisak prsta, retine oka, šake itd.) za otključavanje interfejsa, čime se implementira dvoslojna ili troslojna, *jaka autentifikacija,* koja od korisnika zahteva višekratnu identifikaciju i verifikaciju identiteta. Korisnik nema pristup samom ključu u *smart* kartici i ne može ga otkriti drugom licu, optužujući pri tome da je to uradio neko drugi. Postoje dva glavna tipa smart kartica – *memorijske* i *mikroprocesorske* (kriptokartice).

Memorijske smart kartice se koriste za skladištenje ključa, dok se kriptografske operacije izvršavaju izvan kartice, u aplikaciji na host platformi. *Mikroprocesorske* ili *kriptokartice*, bezbedno skladište ključ i omogućavaju kriptografske operacije na samoj kartici. Aplikacije interaktivno rade sa kriptokarticom preko API *(Application Programming Interface*). Definisano je i standardizovano nekoliko različitih interfejsa (*PKCS#11, PCI, PC/SC, OCF i CDSA),* a izbor zavisi od izvora razvojnog modela. Za zaštitu aplikacija bolje su *kriptokartice*, jer ključevi nikada ne napuštaju bezbedno okruženje, ali pažnju treba obratiti kod implementacije rešenja – PIN ne sme prolaziti kroz OS, što zahteva postojanje eksternog PIN čitača (interfejsa). Ovaj princip ilustrovan je na Sl. 9.7. [74].



Sl. 9.7. Upotreba kriptokartice sa eksternim čitačem kartica

Smart kartice su dobar izbor za zaštitu kriptografskih tajni korisnika, ali nisu pravi izbor za operacije na serverskoj strani, iako se često koriste za skladištenje ključeva administratora za pristup zaštićenom serveru (gde je administrator u ulozi klijenta). Na serverskoj strani bolja opcija je skladištenje ključeva na tzv. **HSM** (*Hardware Security/ Storage Module*). U ovoj oblasti važan standard je NIST FIPS 140–1 i 2 koji pokriva ukupno jedanaest oblasti dizajna i implementacije kriptografskih modula. Standard se koristi za rangiranje bezbednosnih uređaja na četiri bezbednosna nivoa zaštite (1 – najmanji, 4 – najveći). Kriptografski moduli se rangiraju na osnovu serije *zahteva za derivirane testove* (DTR) [67].

Elektronsko poslovanje donosi praktično neograničen broj klijenata, što zahteva veću skalabilnost aplikacija i kriptografskih rešenja zaštite. Za bolje performanse kriptografskih aplikacija koriste se *kriptografski akceleratori* – specijalizovani HSM, koji kombinuju bezbedno skladištenje ključeva sa jakom kriptozaštitom.

9.2.1.7. Ostali autentifikacioni uređaji i protokoli

Biometrika obuhvata tehnike provere *otiska prsta, geometrije ruke, mrežnjače i DNK,* prepoznavanja *govora, lica i facijalne termografije*. Svi mehanizmi zaštite pristupa RM/ RS uvek su kompromis između potrebe za zaštitom i potrebe za komfornim pristupom regularnih korisnika. Biometrijski uređaji verifikuju identitet korisnika na bazi jednog ili više fizičkih atributa, jedinstvenih biometrijskih parametara. Kriterijumi za izbor biometrijskih tehnika mogu biti različiti, kao što su: *performanse i pouzdanost, pogodnost za primenu, kompleksnost korisničke upotrebe, sposobnosti korisnika, korisnička prihvatljivost, troškovi nabavke i dr.* Iako se preporučuje biometrijska autentifikacija korisnika, ovu primenu prate brojni problemi: *visoka cena, korisnička neprihvatljivost,*

visok stepen grešaka, nemoguća autentifikacija uređaja, neotpornost na napade (npr. otisak prsta) i dr.

Tokeni se dele na: *uređaje za bezbedno skladištenje kriptografskih informacija i priručne uređaje za autentifikaciju*. Prvi su alternativa *smart* karticama. Drugi su opremljeni sa malim displejom i tastaturom i generalno se ne moraju povezivati na radnu stanicu. Uređaj se konfiguriše sa autentifikacionim serverom pre izdavanja prava pristupa korisniku, kada server i token razmene kriptografske tajne. Korisnik unosi lozinku ili PIN za pristup tokenu, koji na displeju prikaže autentifikacione podatke potrebne za pristup autentifikacionom serveru. Ove podatke korisnik unosi u svoju radnu stanicu i kompletira proces autentifikacije.

„Metod generisanja ključeva za komunikacionu sesiju šifrovanja i sistem autentifikacije", (patent US Br. 7.577.987, 2009), opisuje novi sistem upravljanja šifarskim ključem, integrisan sa dvoslojnim autentifikacionim protokolom. Ovaj sistem obezbeđuje autentifikaciju strana u vezi, u klijent–server arhitekturi, što omogućava bezbednu distribuciju tajne sesije – simetričnih, slučajnih šifarskih ključeva, generisanih u serveru i distribuiranih klijentima. Velika proliferacija B2B i B2C mreža e–trgovine, koje omogućavaju konekcije korisnika mobilnim uređajima, laptop/desktop računarima, ATM, POS terminalima, VOIP, GPS i drugim uređajima za procesiranje, zahteva poboljšanje infrastrukture zaštite korisnika, posebno u oblasti autentifikacije i zaštite podataka u prenosu.

Upotreba PKI infrastrukture ima izvesna ograničenja za veliki broj korisnika, zbog složenosti uvođenja tehnologije, troškova i administracije ključeva/sertifikata. Ova ograničenja, prevazilazi **MEDIA** protokol (US patent), korišćenjem mehanizama za dvoslojnu uzajamnu autentifikaciju i bezbednu sesiju za distribuciju slučajnog simetričnog ključa. Zaštitu razmene ključeva u **MEDIA** protokolu obezbeđuju algoritmi, zasnovani na sledeće tri tehnologije, ugrađene u proizvod *AuthGard*:

arhitektura za generisanje ključa koja koristi algoritam **TILSA –** (*Time Interplay Limited Session Random Key*) – (US Patent No. 7.577.987),

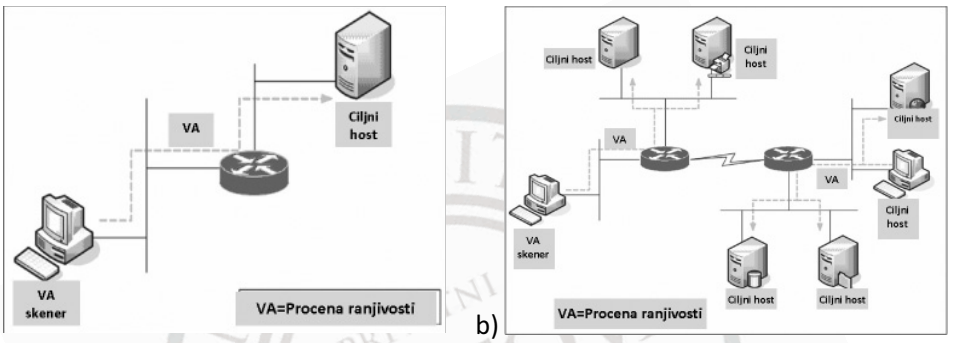
protokol za razmenu ključa koji koristi TILSA algoritam i autentifikacione parametre strana u komunikaciji sa iterativnim algoritmom za ključ za šifrovanje/dešifrovanje – **KEDIA** (*Key Encryption/Decryption Iterative Algorithm*) – (US Patent No. 7.506.161) i

tehnologija za konverziju ključa – **KCA** (*Key Conversion Array*), koja obezbeđuje visok nivo zaštite poruka preko nepoverljivih linija, korišćenjem jednog od patentiranih algoritama – *Bit–Veil–Unveil* (BitVU), *Byte–Veil–Unveil* (ByteVU) i *Bit–Byte–Veil–Unveil* (BBVU) – (US Patent No. 7.299.356).

9.2.2. Zaštita integriteta računarske mreže

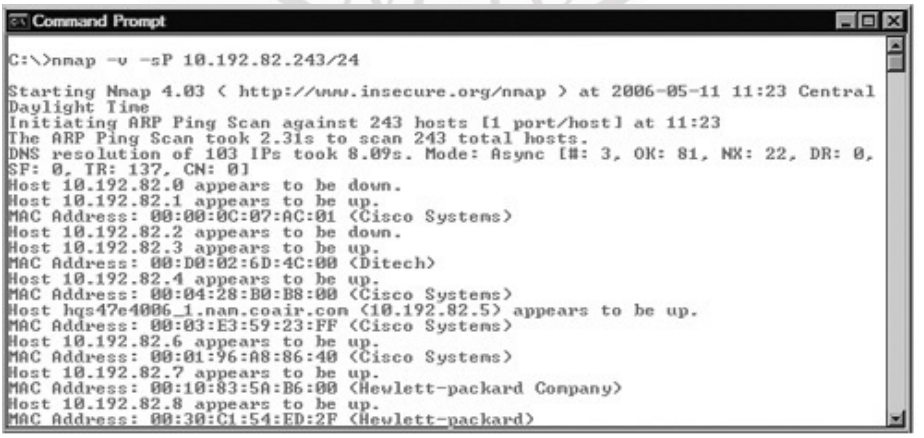
9.2.2.1. Skeneri ranjivosti računarske mreže

Skeneri zaštite integriteta RM po konceptu su slični skenerima zaštite RS, s tim da se otkrivaju ranjivosti RM. Na Sl. 9.8. prikazana je arhitektura tipičnog skenera za procenu ranjivosti RS u mrežnom okruženju i RM.



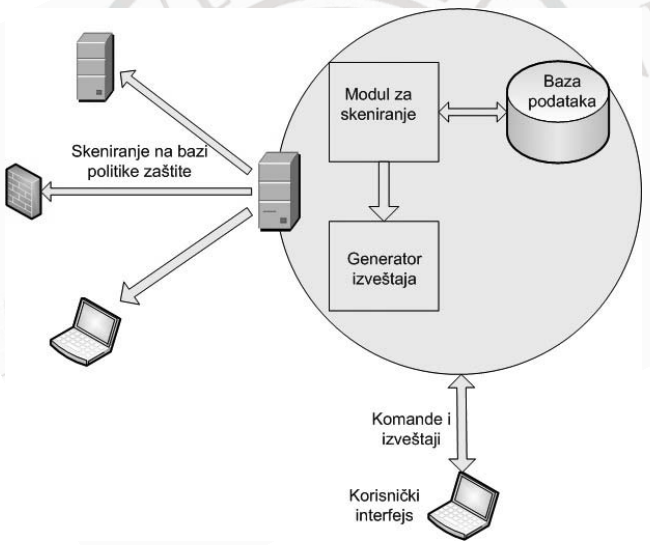
Sl. 9.8. Tipičan skener za procenu ranjivosti RS – (a) i implementacija u RM – (b) [109]

Najjednostavniji skener ranjivosti RM samo mapira uređaje povezane u RM, koristeći jednostavni probni ICMP (*Internet Control Message Protocol*) *eho* signal, poznat kao *ping*. Na Sl. 9.9. prikazan je rezultat *pingovanja* mrežnih uređaja u *Nmap* alatu (*PingSweep*).



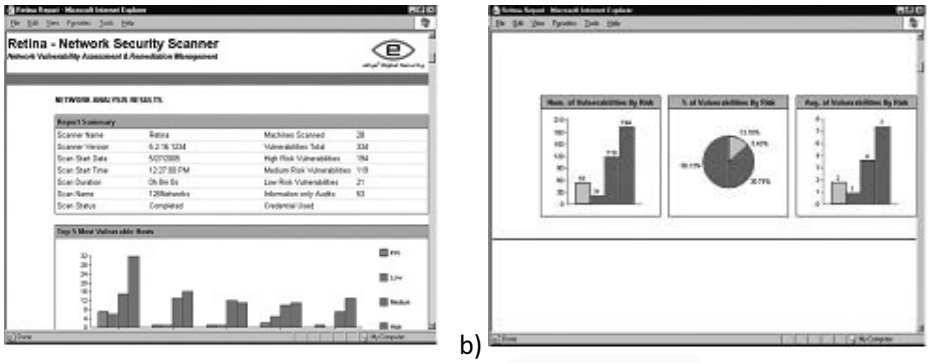
Sl. 9.9. Rezultat pingovanja mrežnih uređaja u Nmap alatu (PingSweep)

Na višem nivou su jednostavni alati koji mogu mapirati portove, pingujući individualne TCP ili UDP portove na detektovanim hostovima. Ovi alati mogu mapirati mrežu i identifikovati koji su mrežni servisi operativni. Komercijalni alati, iako koriste manje više iste tehnike, znatno su moćniji, jer sadrže baze podataka sa poznatim ranjivostima. Mrežni skeneri su bazirani na sličnim principima, kao i host orijentisani (Sl. 9.10), tj. upoređuju aktuelnu konfiguraciju RM i hostova sa predefinisanom referentnom konfiguracijom i izveštavaju o otkrivenim razlikama. Generalno, skeneri RM obezbeđuju više vrsta informacija, ali sa manje detalja od skenera RS. Arhitektura skenera ranjivosti RM uključuje *modul za skeniranje, bazu podataka sa definicijama poznatih ranjivosti, modul za generisanje i prezentaciju izveštaja i korisnički interfejs*. Modul za skeniranje implementira politiku zaštite, koja omogućava prilagođavanje procesa skeniranja zahtevima okruženja, skenira RM, otkriva i poredi tekuće ranjivosti sa poznatim iz baze podataka i daje podatke na izlazu. Rezultati se prikazuju preko korisničkog interfejsa za izveštavanje.



Sl. 9.10. Skeneri ranjivosti računarskih mreža

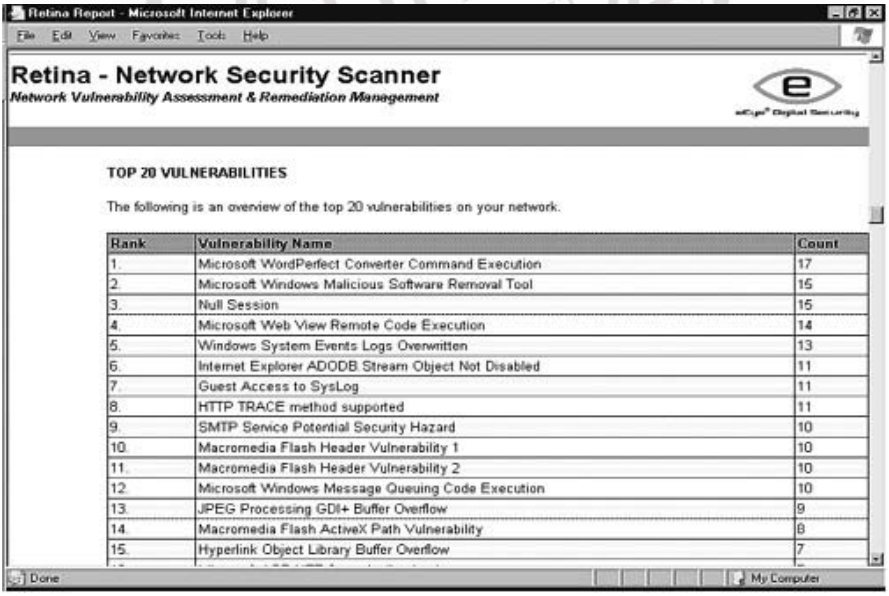
Efektivnost skenera RM zavisi od sličnih faktora kao i skeneri RS: *ažurnosti baza podataka* poznatih ranjivosti; *lokacije skenera* u topologiji RM u odnosu na uređaje, koji mogu blokirati mrežni saobraćaj (barijere, rutere...), što se mora pažljivo planirati; *adekvatnosti politike skeniranja* i *efikasnosti procesa korekcije,* koji sledi po otkrivanju ranjivosti. Poslednji faktor je najvažniji, jer bez otklanjanja uzroka ranjivosti RM proces skeniranja nije završen. Za procenu ranjivosti RM koriste se brojni alati. Na Sl. 9.11a i b prikazani su primer izveštaja o analizi ranjivosti u lokalnoj mreži primenom alata *Retina–Network Security Scanner* (*eEye Digital Security,* www.eEye.com**)**.



a) b)

Sl. 9.11. Rezultati analize ranjivosti – (a) i tipovi izveštaja – (b) u Retina alatu

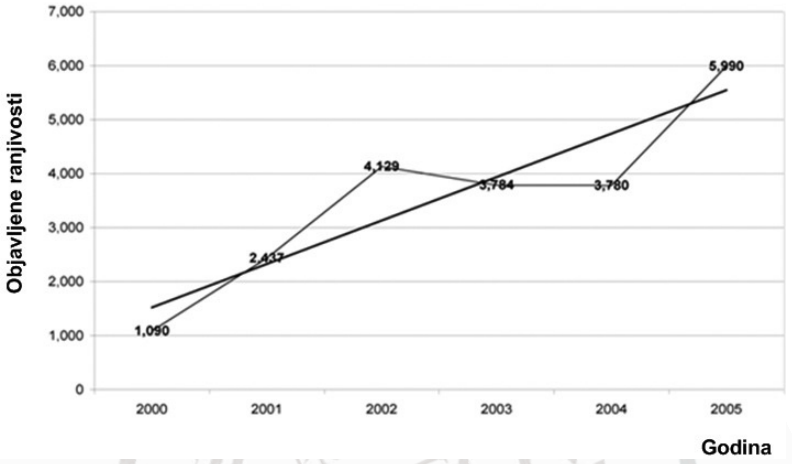
Analitičar zaštite ili menadžer, na osnovu ovih rezultata, mogu brzo proceniti podložnost poznatim bezbednosnim ranjivostima. Na Sl. 9.11a prikazano je 334 ranjivosti na 28 mašina, od kojih se 194 smatra visoko rizičnim. Na Sl. 9.11b ranjivosti su prikazane prema stepenu rizika, procentu zastupljenosti i srednjoj matematičkoj vrednosti broja ranjivosti po kategoriji rizika i hostu. Na Sl. 9.12 prikazane su glavne ranjivosti RM u 2006. godini, otkrivene alatom *Retina–Network Security Scanner* [60].



Rank	Vulnerability Name	Count
1.	Microsoft WordPerfect Converter Command Execution	17
2.	Microsoft Windows Malicious Software Removal Tool	15
3.	Null Session	15
4.	Microsoft Web View Remote Code Execution	14
5.	Windows System Events Logs Overwritten	13
6.	Internet Explorer ADODB.Stream Object Not Disabled	11
7.	Guest Access to SysLog	11
8.	HTTP TRACE method supported	11
9.	SMTP Service Potential Security Hazard	10
10.	Macromedia Flash Header Vulnerability 1	10
11.	Macromedia Flash Header Vulnerability 2	10
12.	Microsoft Windows Message Queuing Code Execution	10
13.	JPEG Processing GDI+ Buffer Overflow	9
14.	Macromedia Flash ActiveX Path Vulnerability	8
15.	Hyperlink Object Library Buffer Overflow	7

Sl. 9.12. Glavne ranjivosti RM (2006) [60]

Od 1995. do 1999. godine, javno je objavljeno samo 1.506 ranjivosti, a samo u 2000. – 1.090. Koristeći podatak iz 2000. godine kao osnovu od kojih su mereni relativni nivoi porasta ranjivosti, od 2005. godine zabeležen je porast od preko 500 ranjivosti godišnje (Sl. 9.13).



Sl. 9.13. Linearna aproksimacija rasta ranjivosti od 2000–2006 [60]

Na Sl. 9.13. prikazane su otkrivene ranjivosti u periodu od 2000. do 2006. godine, sa linearnom aproksimacijom rasta prema jednačini:

$$y=805,6x + 716,6$$

gde je:

y– procenjeni broj ranjivosti za datu godinu, x– procenjeni vremenski period (npr. 2000=1, 2001=2, 2006=7), 805,6 – nagib i 716,6 – y–intercept.

Na bazi ovog trenda procenjen je rast ranjivosti za 2006. i 2007. godini na 6.353 i 7.158, respektivno.

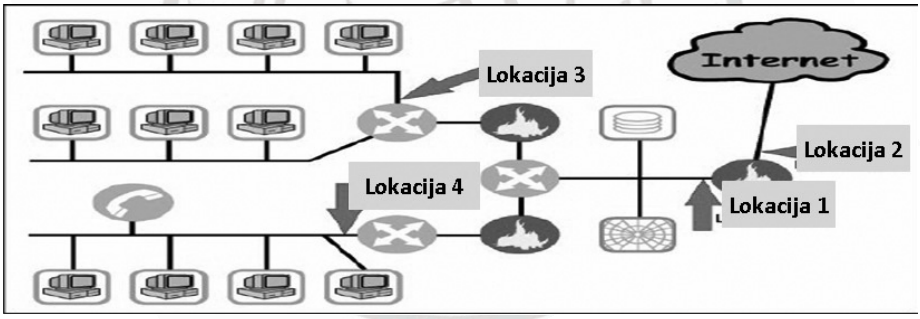
9.2.2.2. Skeneri telefonskih veza

Skeneri telefonskih veza su komercijalni razvoj hakerskih alata tzv. *war dialing* programa, koji se koriste za identifikovanje potencijalnih ranjivosti sistema preko telefonske linije. Konceptualno su sasvim slični skenerima ranjivosti RM; biraju seriju telefonskih brojeva, vrše određeni broj bezbednosnih provera, izveštavaju o rezultatima i na taj način prave bezbednosnu mapu telefonskog sistema organizacije, dok skeneri ranjivosti RM mapiranjem IP adresa prave mapu uređaja lokalne mreže. Detektuju ranjive puteve

u RM, koji su pristupačni sa javne telefonske mreže i nepoznate modeme u LAN-u. Kombinuju tehnike *pingovanja* i *prompts* za izveštavanje o ranjivostima OS (npr. slaba lozinka) i na nivou aplikacija (npr. udaljeni pristup bez lozinke). U većini slučajeva poseduju jednostavan GUI i proizvode nekoliko različitih tipova *kastomizovanih* izveštaja.

9.2.3. Mehanizmi za detekciju i sprečavanje upada u mrežu

Mrežni sistemi za detekciju (NIDS) i sprečavanje upada (NIPS) – NIDPS, u većini slučajeva rade na 2. sloju OSI modela. Programska rešenja u NIDPS stavljaju mrežnu karticu (NIC) u *promiskuitetni* režim rada, privilegovanu operaciju na većini NIDPS sistema, koja daje pristup mrežnom saobraćaju u realnom vremenu. Na sličan način rade i analizatori mreže i *sniferski* programi. NIDPS sistemi su komplementarni HIDPS sistemima po mogućnosti prijema i analize informacija, ali ne i po protokolima koji nisu na raspolaganju HIDPS sistemu. Pošto rade na mrežnom sloju, NIDPS detektuju sisteme nezavisno od OS i omogućavaju zaštitu velikog opsega krajnjih platformi. Mogućnosti aplikacije NIDPS sistema u RM prikazana je na Sl. 9.14., a prednosti instalacije NIDPS na različitim lokacijama u RM date su u Tabeli 9.4. [2, 87].



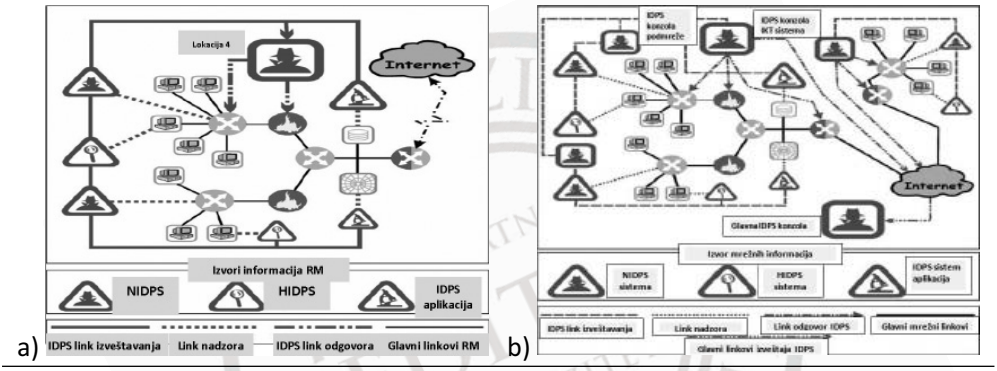
Sl. 9.14. Mogućnosti primene NIDPS sistema u RM [87]

Tabela 9.4. Zbirne prednosti instalacija NIDS na različitim lokacijama u RM

Lokacija	Prednost
1. DMZ	Vidi napade sa Interneta koji probijaju odbranu spoljnog perimetra RM.
	Ističu probleme sa politikom, ili funkcionisanjem mrežne *barijere.*
	Vidi napade na *web,* ili *FTP* server, koji su obično smešteni u DMZ.
2. Izvan barijere	Dokumentuje broj napada koji potiču sa Interneta, a pogađaju RM.
	Dokumentuje tipove napada koji potiču sa Interneta, a pogađaju RM.

Lokacija	Prednost
3. Na RM sabirnici	Monitoriše mrežni saobraćaj i povećava mogućnost detekcije napada.
	Detektuje neovlašćene aktivnosti legalnih korisnika iz RM organizacije.
4. Na kritičnoj submreži	Detektuje napade usmerene na kritične IKTS i kritične objekte IKTS.
	Usmerava ograničen resurs zaštite na najvrednije mrežne objekte.

Na Sl. 9.15. prikazane su blok šeme centralizovanog (a) i distribuiranog (b) upravljanja NIDPS sistemom.



Sl. 9.15. Upravljanje NIDPS sistemima: centralizovano – (a) i distribuirano – (b) [87]

Zbog sličnosti načina rada sa barijerom, NIDPS imaju i nekoliko sličnih ograničenja. Barijera treba da razume i prepozna protokol da bi donela odluku o pristupu na bazi informacija koje sadrži, a NIDPS program ne može detektovati anomalije protokola bez takvog razumevanje. Očigledno, ni barijere ni NIDPS sistemi ne mogu interpretirati podatke. Svaka arhitektura sistema zaštite koja kombinuje barijere, kriptozaštitu i NIDPS, treba da uzme u obzir ovo ograničenje [89].

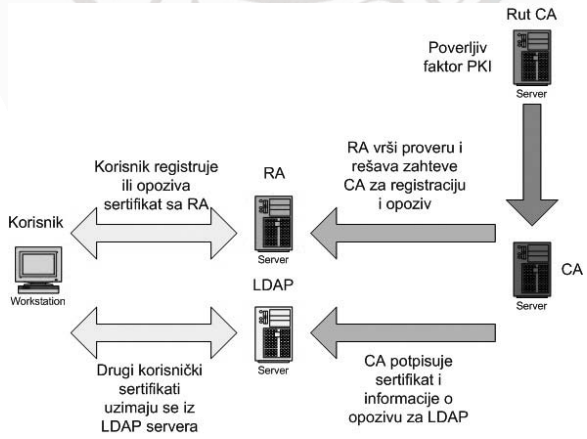
NIDPS program može igrati važnu ulogu u upravljanju malicioznim kodovima, tako što se može konfigurisati da prepozna određene potpise i preduzme neke predefinisane akcije, posebno u periodu između inicijalnog napada i raspoloživosti prve definicije malicioznog kôda. NIDPS program, takođe, može biti konfigurisan da sprečava prolaz inficiranih objekata izvan organizacije, što je koristan mehanizam za sprečavanje širenja malicioznih programa na druge hostove izvan organizacije. Odgovor NIDPS sistema može biti identifikacija i logovanje događaja, neka aktivna protivmera ili kombinacija ove dve. Pasivna tehnika upozoravanja uključuje izveštavanje o problemu na ekranu monitora, generisanje SNMP (*Simple Network Management Protocol*) alarma, aktiviranje mobilnog telefona i sl. Aktivne mere zaštite treba pažljivo implementirati, pošto mogu izazvati prekid servisa posebno u slučaju lažnih pozitiva, jer ukidaju konekcije u interakciji sa barijerom.

9.2.4. Infrastrukturni mehanizmi za zaštitu računarske mreže

9.2.4.1. Infrastruktura sa javnim ključem (PKI)

PKI je koherentna implementacija T, O i U kontrola zaštite, koja omogućava stranama u transakciji poverenje u povezanost Pk i njegovog vlasnika, što garantuje CA. Mera u kojoj se korisnik može osloniti na ovu povezanost zavisi od *kvaliteta procesa* sa kojim CA izdaje DS i verifikuje identitet korisnika sertifikata. Generalno, PKI ništa ne govori o poverenju korisnika u DS. Iako se bezbednosnom proverom, pre izdavanja sertifikata, može obezbediti neki nivo poverenja između korisnika, ova praksa nije obavezna za CA. Da bi korisnici imali poverenje u DS, CA opisuje praksu i procese, koje koristi za izvršavanje dnevnih poslova u *Izjavi o praksi sertifikacije* – **CPS** (*Certificate Practice Statement*). Pravila i ograničenja korišćenja svakog posebnog tipa DS definisana su u dokumentu *Politika sertifikacije* – **CP** (*Certificate Policy*). U ovoj oblasti postoji dosta zrelih standarda i uputstava, ali nažalost svi nisu koherentni [5, 58, 74].

Osnovni moduli PKI sistema za većinu implementacija uključuje **CA,** *Telo za registraciju* **– RA** (*Registration Authority*) i **Imenik** (*Directory*). Termin **CA** se koristi istovremeno za opis entiteta, koji upravlja i administrira PKI sistem i komponente zaštite za izdavanje i upravljanje DS. Korektna interpretacija je obično evidentna iz konteksta. PKI sistem može implementirati i dodatne module, kao što su *hardversko softverski modul (***HSM***), smart kartice i tokeni, kriptografski akceleratori* za ubrzavanje performansi, **OCSP** *(Online Certification Status Protocol)* responder za verifikaciju statusnih informacija o DS u realnom vremenu*, programi za validaciju transakcija* i drugi programi za podršku. Glavni PKI moduli u interaktivnom radu prikazani su na Sl. 9.16.



Sl. 9.16. Ključni moduli PKI sistema

U *imeniku,* tipa X500 ili LDAP *(Lighweight Directory Access Protocol)* servera, čuvaju se statusne informacije o aktivnim i opozvanim DS. Aplikacije razvijene za PKI sistem koriste jednostavan *LDAP* protokol*,* za pristup *Imeniku* i izvlačenje informacija o DS. Detaljniji opis funkcionalnosti CA i RA dat je u Tabeli 9.5.

Tabela 9.5. Funkcionalnosti CA i RA

CA	Prihvata potvrđene zahteve za generisanje i povlačenje DS od RA i operatera CA – CAO (*Certification Authority Operator*) i isporučuje DS i potvrdne poruke.
	U skladu sa politikom, dostavlja krajnjim korisnicima par javnih i privatnih ključeva za šifrovanje/dešifrovanje koji su označeni da se arhiviraju u bazi ključeva.
	Digitalno potpisuje sertifikate krajnjih korisnika i sertifikate podređenih CA, kao i drugih CA, u slučaju unakrsne sertifikacije (*cross–certification*).
	Digitalno potpisuje sve informacije objavljene u listi za opoziv sertifikata – CRL (*Certificate Revocation List*) i opoziv drugih CA – ARL (*Authority Revocation List.*).
	Digitalno Potpisuje sve poruke koje CA šalje i koje se razmenjuju preko CA u PKCS#7 formatu.
	Verifikuje sve poruke koje dobije u cilju provere autentičnosti i zaštite integriteta.
	Digitalno potpisuje sve relevantne podatke, informacije i log datoteke, arhivirane u bazi podataka CA; svaki ulazak u bazu poseduje odgovarajući jedinstveni broj.
	Opciono publikuje DS, CRL i ARL na LDAP ili X.500 direktorijumu, kao i na HD.
	Opciono može publikovati CRL i na OCSP (*Online Certification Status*) serveru.
	Generiše svoj par ključeva za asimetrični kriptografski algoritam i za CAO.
	Opciono proverava da li svi izdati sertifikati imaju jedinstveni *Dname* i javni ključ.
RA	Zahteve za izdavanjem ili povlačenjem DS, koje RAO potvrdi, prosleđuje do CA; prima DS i potvrdne poruke od CA i prosleđuje do RAO.
	Prosleđuje *web* zahteve za izdavanjem ili povlačenjem DS (preko *gateway–a)* do RAO i dostavlja sertifikate i informacione poruke nazad *gateway–u*.
	Digitaln Potpisuje sve poruke koje šalje RA.
	Procesira sve dobijene, digitalno potpisane poruke – verifikuje DP, autentičnosti potpisnika i integritet sadržaja poruke.
	Sve poruke koje se razmenjuju preko RA šifruje u PKCS#7 formatu.
	Sve podatke i log datoteke digitalno potpisuje i arhivira u bazi podataka RA; svaki ulazni slog ima jedinstveni broj procesiranja.
	Autentifikuje mreže krajnjih korisnika u slučaju udaljene registracije preko *web*–a.
	Vrši inicijalizaciju i distribuciju hardverskih uređaja (smart kartica, tokena, HSM).
	Generiše i upravlja ključevima, kontroliše registrovane izmene.
	Izveštava o aktivnostima registrovanja i opoziva sertifikata.
	Od RAO ili preko *web*–a prihvata zahteve za registraciju, izdavanje i/ili opoziv DS.
	Verifikuje ove informacije i dodatno proverava identitet – posedovanje Pk.
	Prihvata ili odbija zahteve; DS ili informacije o opozivu DS prosleđuje CA–u na potpisi; ako je zahtev odbijen obaveštava korisnika.
	Registruje u repozitorijumu izdati sertifikat i prosleđuje korisniku kopiju, koju potpiše CA; objavljuje informacije o opozivu sertifikata po planu.

Generalno, arhitektura složenog PKI sistema može imati *hijerarhijsku, rešetkastu i tranzicionu* (*bridge*) strukturu organizacije CA.

Hijerarhijska struktura PKI podrazumeva razvoj i implementaciju *rut CA,* koje je stub poverenja ove infrastrukture. Obično je na nacionalnom nivou, ima samo-potpisani DS, strogo čuva Tk, a Pk objavljuje u više raspoloživih baza, da bi obezbedio nekoliko referentnih i redundantnih izvora. Izdaje i potpisuje DS, uslovljava tehnologiju, metode rada i politiku drugih CA, koji u svojim domenima zaštite potpisuju DS korisnika ili nižih CA, u višeslojnoj hijerarhijskoj strukturi. Podređeni CA ne izdaje DS rut sertifikacionom telu. Rut CA ograničava dubinu hijerarhije, što je i osnovni nedostatak *ove arhitekture*. Dubina hijerarhije definiše koliko nižih CA može biti formirano ispod rut CA, što postaje suviše kompleksno za velike PKI sisteme. Bezbednost hijerarhijske strukture u celini zavisi od tajnosti Tk rut CA. Rut CA ne mora nužno biti na vrhu hijerarhijske arhitekture PKI, ali mu svi korisnici veruju. Sertifikacioni put je jednosmeran i počinje sa Pk rut CA nadole. *Glavne prednosti* su jednostavna struktura, jednosmeran put poverenja i centralno upravljanje. DS je manji i jednostavniji, a struktura skalabilna – rut CA iz PKI1 može se povezati sa rut CA iz PKI2 ili podređenim CA iz PKI2. Sertifikacioni put se lako se razvija i relativno je kratak – **najduži put = dubini stabla + 1**. Korisnici iz sadržaja DS implicitno znaju za koje se aplikacije DS može koristiti. *Glavni nedostatak* je oslanjanje na jednu tačku poverljivosti – Tk rut CA i ako dođe do kompromitacije ugrožena je cela PKI struktura. Ne postoji neposredna procedura tehničkog oporavka. Takođe, sporazum nekih korisnika samo sa jednim rut CA može biti politički onemogućen, tranzicija od seta izolovanih CA logistički nepraktična i teže upravljanje za veće PKI sisteme.

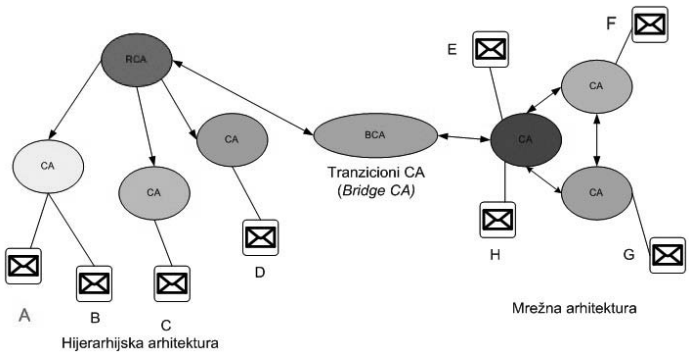
Rešetkasta struktura direktno povezuje pojedinačna CA i sva CA su poverljive tačke. CA razmenjuju sertifikate jedni sa drugima (unakrsna sertifikacija), pa je put poverljivosti dvosmeran. Ove sertifikate izdaje jedno CA koje poseduje privatni ključ (Tk), a Pk se prosleđuje svim CA u mreži. Unakrsnim DS veruju svi CA u mreži. *Glavne prednosti* su uzajamna distribucija poverenja na sve CA, direktna povezanost pojedinačnih CA i dvosmeran put poverenja. *Glavni nedostaci* su visoki troškovi uspostavljanja i uslovljenost poverenja, gde neko CA može ograničiti poverenje, specifikacijom u DS. Zato je izgradnja puta poverenja neodređena, a sertifikacioni put kompleksniji. Maksimalna dužina sertifikacionog puta je broj CA u mreži. U slučaju kompromitacije, oporavak je teži i kompleksniji, jer postoji mogućnost stvaranja beskonačne petlje DS. Aplikacija DS se određuje na bazi sadržaja, a ne lokacije CA u PKI strukturi. Ova arhitektura zahteva veće i kompleksnije sertifikate i kompleksnije procesiranje sertifikacionog puta. Generalno, glavni kriterijumi za uspostavljanje PKI sistema na nacionalnom nivou su *integrisanje postojećih arhitektura bez bitnih modifikacija istih, uspostavljanje najlakšeg puta za sticanje poverenja u digitalno potpisane poruke i zahtev za globalnom interoperabilnosti nacionalnih PKI sistema*. Za globalnu konfiguraciju PKI sistema prva dva modela ne odgovaraju, zbog relativne izolovanosti, kompleksnosti i teškoće definisanja rut CA u hijerarhijskoj arhitekturi i visoke kompleksnosti mrežne arhitekture za složene PKI sisteme na nacionalnom nivou.

Tranzicione arhitektura – BCA (*Brige CA)* je kritičan faktor uspeha za inter-operabilnost nacionalnih PKI na globalnom nivou. U suštini BCA je, za druge PKI arhitekture, rešetkasta arhitektura sa *habom* ili hijerarhijska arhitektura sa spoljnom vezom. BCA ne izdaje DS direktno korisnicima i u tom smislu nije poverljivi entitet za korisnike PKI. BCA je fleksibilan mehanizam, koji povezuje različite PKI arhitekture. Poverenje se prenosi prema modelu zvezde gde je nacionalni BCA centar poverenja. Korisnici koriste svoje vlastite i samopotpisane CA kao osnovne tačke poverenja, umesto manje poznatog rut CA. Dakle, poverenje se gradi sa vlastitim CA kroz BCA, koje može da *izdaje DS* ("*a la rut CA*") glavnim CA (*principalima*) ili *listu poverljivih CA,* umesto DS.

Primer 1: *EU BridgeCA*, *Nemačka banka, Telekom i TeleTrust* BCA izdaju DS glavnim CA, koji su potpisani sa Pk BCA, objavljenim na sajtu BCA. Korisnici tipično znaju put do BCA i treba da odrede put od BCA do drugih korisnika DS. Dužina sertifikacionog puta duplo je veća od hijerarhijskog, ali decentralizovana struktura BCA mnogo preciznije modeluje realne odnose organizacija.

Primer 2: BCA ne izdaje DS nego *listu poverljivih CA* (TL), potpisanu sa Pk BCA, sa informacijama o njihovom statusu (objavljen je italijanski standard *ETSI TS102 231* za harmonizaciju statusnih informacija o CA). U tom slučaju korisnici mogu sami odlučiti kojem će CA sa liste ukazati poverenje.

Glavne prednosti BCA arhitekture su lakši oporavak puta poverenja nego u mrežnoj, a teži nego u hijerarhijskoj arhitekturi i što krajnji korisnici mogu koristiti postojeće DS (do opoziva) i nemaju promena konfiguracije sistema. Glavni *nedostaci* su što korisnici BCA sertifikata sami moraju uspostaviti hardversko-softversku infrastrukturu za BCA sertifikate i poslovne procese, uvesti u upotrebu DS i obučiti korisnike. BCA koji izdaje CA, ne daje detaljnije informacije o statusu CA, što rešava modifikovani BCA sa listom poverljivih CA. Na Sl. 9.17. prikazan je funkcionalni model globalne arhitekture interoperabilnih, nacionalnih PKI sistema.



Sl. 9.17. Model globalne arhitekture PKI sistema

Zaštita integriteta u mrežnom okruženju uključuje zaštitu integriteta *podataka i sesije komunikacije*. Koncept *integriteta podataka* je razumljiv – obezbediti da podaci stignu na odredište neizmenjeni. Integritet podataka štite protokoli, tehnikom uzimanja sažetka podataka (*heša* ili *message digest –MD)*. *Heš* je jednosmerna matematička funkcija, koja se lako računa u jednom, a teško ili praktično nikako u inverznom smeru. *Heš* algoritam od jedinice podataka promenljive veličine stvara sažetak podataka, čija je vrednost fiksne veličine; daje istu *heš* vrednost na osnovu istih ulaznih podataka, odnosno, dve različite ulazne veličine nikada nemaju istu *heš* vrednost. *Heš* podaci se mogu porediti sa otiskom prsta neke osobe. Otisak prsta je jedinstven za tu osobu i relativno fiksne veličine, ali ni približno nije velik kao ta osoba. Heš je jedinstven identifikator, koji je praktično nemoguće dobiti sa drugačijim ulaznim podacima, a deo je svih podataka koje predstavlja. Uobičajeni heš algoritmi koji se najviše koriste su: *MD4* **–** izračunava 128-bitni heš, vrlo je brz i srednje snage [5]; *MD5* **–** 128-bitni heš, brz, bezbedniji od *MD4*, široko primenjen; *SHA–1 (Secure Hash Algorithm)*–160–bitni heš, sporiji od MD5, standardan u federalnom IKTS vlade SAD i *SHA–256, SHA–384, SHA–512, SHA–1024 i SHA 2048 (u* razvoju) [25].

Pošiljalac poruke pravi *heš* poruke sa određenim ključem, koji se naziva kôd za proveru autentičnosti poruke – MAC (*Massage Authentication Code*), a primalac verifikuje *heš* vrednost sa istim ključem. Ako se dobije ista vrednost heša, poruka je nepromenjena.

Integritet sesije obezbeđuje zaštitu komunikacione sesije od bilo koje izmene. Tehnike zaštite su obično zasnovane na uključivanju brojeva sekvenci ili vremenskog pečata u zaštićenoj poruci. Koriste se asimetrični algoritmi u kombinaciji sa heš funkcijama i digitalnim potpisom. *Digitalni potpis pošiljalac pravi hešovanjem teksta poruke i šifrovanjem te vrednosti sa* **Pk** *primaoca*. Primalac dešifruje šifrovanu heš vrednost poruke sa svojim **Tk** i verifikuje heš vrednost sa MAC. Ako se dobije ista vrednost heša, sesija je nepromenjena.

Servis neporicanja sprečava učesnike u transakciji da kasnije poriču izvršene akcije. Mnogo je teže sprečiti primaoca poruke da porekne prijem poruke, nego pošiljaoca da porekne da je poruku poslao. Da bi dokazao da je pošiljalac poslao određenu poruku, primalac mora zahtevati da pošiljalac sistematski digitalno potpisuje poruke pre slanja. Ako pošiljalac kasnije pokuša da porekne slanje poruke, primalac jednostavno proizvede i verifikuje digitalno potpisanu poruku kao neporeciv dokaz da je pošiljalac zaista poslao određenu poruku. Ako pošiljalac želi dokaz da je primalac primio određenu poruku, mora zahtevati da primalac sistematski generiše potvrde o prijemu za svaku poslatu poruku i da je digitalno potpisuje. Ako primalac kasnije pokuša poreći da je primio poruku, pošiljalac proizvede i verifikuje digitalno potpisanu potvrdu o prijemu. Treba zapaziti da je ovde bitno razlikovati čitanje poruke od prijema poruke.

Zaštita poverljivosti mrežnih podataka i informacija postiže se korišćenjem PKI sistema za razmenu simetričnog ključa za šifrovanje, koji se često naziva *sesijski* ključ. Postoje dve osnovne tehnike za sporazumevanje o sesijskom ključu: *korišćenje pro-*

tokola za uspostavljanje ključa (npr. *Diffie –Hellman*) i *generisanje simetričnog ključa, šifrovanje sa Pk udaljenog korisnika* i *transfer asimetričnim PKI sistemom* [5]. Kombinuju se prednosti asimetričnih i simetričnih algoritama. Asimetrični algoritmi se koriste za distribuciju simetričnog ključa, a simetrični - za šifrovanje. Za zaštitu komunikacije dve poverljive RM kroz nepoverljivi Internet, koriste se *virtuelne privatne mreže* – **VPN** (*Virtual Private Networks*). VPN veze su šifrovane upotrebom **IPsec** protokola zaštite i mogu se koristiti na privatnim i javnim mrežama. VPN vezu prave dva VPN servera ili VPN klijent i VPN server. Da bi realizovali šifrovanu vezu, dva uređaja koriste dogovoreni metod šifrovanja. Ako VPN implementiraju dva servera, omda se šifruje komunikacija između dve tačke [26].

9.2.4.2. IPSec protokol

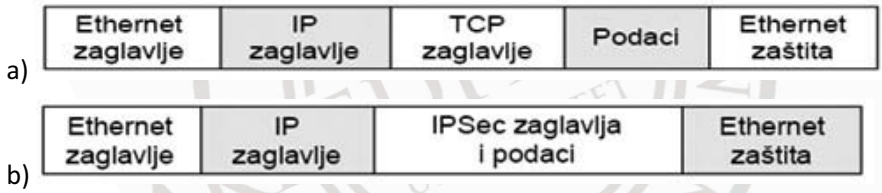
Distribuirani IKTS se štiti od spoljnih napada, upotrebom *mehanizama zaštite komunikacione opreme, mrežnih barijera, NOSSS zaštite na mrežnom nivou i fizičke zaštite pristupa ruterima i serverima*. Zaštitu na mrežnom nivou obezbeđuju mehanizmi za autentifikaciju i zaštitu integriteta i tajnosti IP paketa između mrežnih čvorova. Autentifikacija i zaštita integriteta IP paketa, najčešće se realizuje primenom kriptografskih kompresionih funkcija, upotrebom tajnog ključa – *MAC*, heš funkcija i DS, dok se zaštita tajnosti ostvaruje primenom simetričnih algoritama. Najpoznatiji protokol zaštite na mrežnom nivou je **IPSec** protokol (*Internet Protocol Security*) [26].

Većina RM, uključujući i Internet, za komunikaciju koristi TCP/IP skup protokola. TCP protokol je zadužen za prenos podataka, a IP – za usmeravanje paketa podataka kroz mrežu, od izvorišta do odredišta. IP skup protokola pokazuje dobra komunikacijska svojstva, skalabilnost, prilagodljivost i otvorenost prema različitim arhitekturama i mrežnoj opremi, ali ne obezbeđuje CIA prenošenih podataka. Prenos osetljivih podataka u IP mrežama potrebno je obezbediti na transportnom i aplikativnom nivou. Primer bezbednosnog mehanizma, koji deluje između aplikativnog i transportnog sloja je SSL protokol. Problem je, što postoji veliki broj različitih protokola sa aplikativnog nivoa, za koje je potrebno posebno razvijati mehanizme zaštite.

IPSec protokol je nastao kao rezultat inicijative da se razvije jedinstveni bezbednosni mehanizam za zaštićeni prenos podataka u IP mrežama. Razvila ga je grupa IETF (*Internet Engineering Task Force*), kao proširenje osnovnog IP protokola. IPSec protokol je deo mrežnog sloja, čiji je zadatak prikupljanje podataka o stanju mreže i usmeravanje paketa podataka između mrežnih čvorova. Mrežni sloj koristi funkcionalnosti fizičkog i sloja veze podataka, dok za usmeravanje paketa koristi vlastitu logiku. U IP mrežama ovaj sloj se naziva IP sloj, a usmeravanje paketa kroz mrežu se obavlja prema IP protokolu. Značajno svojstvo IP mreža je potpuna homogenost mrežnog, odnosno IP sloja, dok u ostalim slojevima postoji određen stepen raznovrsnosti. IP sloj koristi jedinstveni IP protokol. Svojstvo homogenosti IP sloja bitno pojednostavljuje uvođenje jedinstvenog bezbednosnog

mehanizma u IP mreži. Zaštitom komunikacije na nivou IP protokola štiti se celokupna mrežna komunikacija. Protokol za zaštitu komunikacije u mrežnom, odnosno IP sloju, naziva se IPSec protokol.

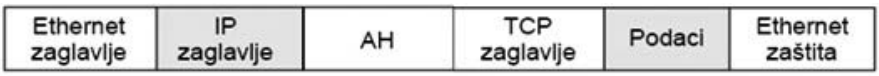
IPSec protokol zadržava kompatibilnost s postojećim IP protokolom, što omogućava transparentnost mrežne opreme, zasnovane na IP protokolu, odnosno, samo dva krajnja učesnika u komunikaciji, moraju imati podršku za komunikaciju IPSec protokolom, dok mrežna čvorišta i ruteri ne moraju imati ovu podršku. Fizički sloj i sloj veze podataka koriste Ethernet zaglavlje i Ethernet zaštitu. Za pravilan rad mrežnog sloja i IP protokola bitno je IP zaglavlje, u kojem su, između ostalog, upisane izvorišna i odredišna adresa IP paketa, koje su potrebne za usmeravanje paketa kroz mrežu. Ostali delovi TCP/IP paketa, pripadaju višim slojevima i za IP sloj predstavljaju obične podatke koje je potrebno preneti kroz mrežu. Da bi se zadržala kompatibilnost IPSec sa IP protokolom, potrebno je, da u strukturi IPSec paketa podataka, ostane očuvano IP zaglavlje. *IPSec protokol stoga obavlja kriptografske akcije nad zaglavljima i podacima viših slojeva*. Polje sa IPSec zaglavljem i podacima uključuje, u šifrovanom obliku, TCP zaglavlje, kao i sva ostala zaglavlja i podatke viših slojeva. Na Sl. 9.18. prikazana je kompatibilnost IP i IPSec protokola za komunikaciju preko Ethernet mreža.



Sl. 9.18. Struktura paketa podataka za prenos putem Ethernet mreža: IP – (a) i IPSec – (b)

Za zaštitu poverljivosti, integriteta, autentičnosti i neporecivosti prenošenih podataka, IPSec koristi tri potprotokola, koja se razlikuju po vrsti IPSec zaglavlja i podataka i to: *zaglavlje za autentifikaciju, enkapsulirani šifrovani podaci i zaglavlje za razmenu ključeva*.

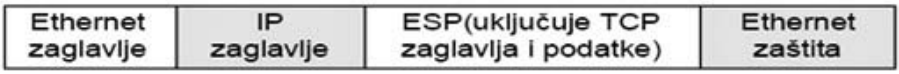
Zaglavlje za autentifikaciju – AH (*Authentication Header*) koristi se za proveru identiteta pošiljaoca podataka i otkrivanje narušavanja integriteta podataka tokom prenosa kroz mrežu (Sl. 9.19).



Sl. 9.19. Struktura IPSec paketa podataka uz korišćenje AH potprotokola u Ethernet mreži

Izvodi se metodom digitalnog potpisivanja podataka. Ovo zaglavlje ne čuva tajnost podataka i koristi se samo u slučajevima kada je bitna autentičnost i integritet podataka. Potprotokol za autentifikaciju može biti primenjen kao samostalni potprotokol IPSec protokola ili u sprezi sa ESP potprotokolom. Samostalni AH potprotokol osigurava autentičnost i integritet prenošenih podataka, dok sprega AH i ESP potprotokola osigurava autentičnost, integritet i tajnost prenošenih podataka. Razlika između AH potprotokola i polja podataka za autentifikaciju kod ESP potprotokola je u tome što AH potprotokol, osim ESP polja ili TCP paketa, ako se ne koristi ESP, digitalno potpisuje i IP zaglavlje. Da bi se uvek osigurao minimalni nivo autentifikacije, predloženo je da sve verzije AH potprotokola za digitalno potpisivanje podataka koriste MD5, SHA1, SHA2 i druge algoritme.

Enkapsulirani šifrovani podaci – *ESP* (*Encapsulating Security Payload*) IPSec paketa, koriste se kada je bitnije očuvati tajnost prenošenih podataka (Sl. 9.20).



Sl. 9.20. Struktura IPSec paketa uz korišćenje ESP potprotokola u Ethernet mrežama

Za stvaranje ESP polja podataka koriste se simetrična kriptografija, u sprezi s metodom digitalnog potpisa podataka. ESP potprotokol čuva tajnost podataka, primenom nekog simetričnog kriptografskog algoritma na sadržaj IP paketa. Za minimalni nivo zaštite predložen je standardni 56–bitni DES algoritam. Sastavni delovi ESP polja su *indeks bezbednosnih parametara* – **SPI** (*Security Parameter Index*), *redni broj paketa*, *korisni podaci, dopuna do punog bloka, veličina dopune do punog bloka i oznaka protokola,* koji sledi nakon ESP polja.

SPI je 32–bitni jednoznačni broj, kojim su određeni kriptografski algoritmi, ključevi, trajanje ključeva i ostali bezbednosni parametri, korišćeni u komunikaciji. Primalac ga koristi da dešifruje podatke sa istim parametrima, kojim su i šifrovani. *Redni broj* paketa, uvećava brojač paketa za jedan, prilikom svakog slanja paketa na istu odredištu adresu, uz korišćenje istog SPI. Koristi se da bi se paketi na odredištu mogli pravilno poređati, kao i za sprečavanje napada ponavljanjem istih paketa. *Korisni podaci* su stvarna korisna informacija, koja se prenosi mrežom. *Dopuna do punog bloka* (*Padding*) je količina od 0 – 255 bajtova, koji se dodaju, da bi se blok korisnih podataka dopunio do veličine punog bloka, koju koristi kriptografski algoritam. Veličina dopune do punog bloka (*Pad Length*) sadrži podatak o broju bajtova, koji su dodati za dopunjavanje korisnih podataka do punog bloka. Oznakom protokola, koji sledi nakon ESP polja (*Next Header*), naznačava se prisustvo podataka za autentifikaciju na kraju ESP polja. Podaci za autentifikaciju nisu obavezni deo ESP polja i mogu se izostaviti. Oznaka protokola označava da li su podaci za autentifikaciju sastavni deo ESP polja. Prva dva dela u ESP polju, SPI i redni broj paketa,

kroz mrežu se prenose u otvorenom obliku, jer su potrebni primaocu, pre nego što obavi dešifrovanje, a ostali delovi se šifruju. Nakon oznake protokola, može se nalaziti polje sa podacima za autentifikaciju, odnosno, digitalni potpis korisnih podataka, čija dužina zavisi od korišćenog algoritma. Digitalno se potpisuju svi prethodno navedeni delovi ESP polja, uključujući i SPI i redni broj paketa. ESP polje se digitalno potpisuje sa MD5, SHA–1 ili SHA–2 algoritmom, nakon što se korisni podaci šifruju.

Zaglavlje za razmenu ključeva – *IKE* (*Internet Key Exchange*) koristi se u potprotokolu za razmenu ključeva, a služi za dogovaranje bezbedonosnih parametara IPSec komunikacije i razmenu simetričnih ključeva. IKE se prilagođava uspostavljanju metoda autentifikacije, kriptografskih algoritama i dužine ključeva, kao i načinu razmenu ključeva između učesnika komunikacije. Za dogovaranje parametara bezbedne komunikacije, IKE potprotokol uvodi koncept bezbednosne asocijacije – *SA* (*Security Association*), predstavljene SPI indeksom. *SA* objedinjuje sve podatke, potrebne učesnicima za komunikaciju IPSec protokolom; definiše vrstu i način rada algoritma za digitalno potpisivanje podataka i korišćenih ključeva; definiše vrstu i način rada kriptografskog algoritma za šifrovanje podataka ESP potprotokola; definiše sprovođenje ili izostavljanje postupka sinhronizacije kod kriptografskih algoritama, parametre sinhronizacije, protokol za utvrđivanje autentičnosti podataka (AH ili ESP), životni vek i učestalost promene ključeva, životni vek i izvorišne adrese *SA* i stepen osetljivosti prenošenih podataka. *SA* se može smatrati vrstom sigurnog komunikacijskog kanala kroz rizično mrežno okruženje, između učesnika koji komuniciraju IPSec protokolom.

Servisi i mehanizmi mrežne zaštite zbirno su prikazani u Tabeli 9.6.

Tabela 9.6. Servisi i mehanizmi mrežne zaštite

Mehanizam / Servis	Kz	DS	AC	Integritet podataka	Aut.	Pading saobraćaja	Kontrola saobraćaja	Notorizacija
Aut. entiteta	x	x			x			
Aut. izvora podataka	x	x						
AC			x					
Pov. podataka	x						x	
Pov. toka saobraćaja	x					x	x	
Integritet podataka	x	x		x				
Neporecivost		x		x				x
Raspoloživost				x	x			

Legenda: Aut. – autentifikacija; **AC** – kontrola pristupa; **Pov.** – poverljivost; **Kz** – šifrovanje; **DS –** digitalni potpis; **Pading saobraćaja** – ubacivanje bita u prazne prostore niza podataka radi otežavanja prisluškivanja; **Notorizacija** – korišćenje poverljivog provajdera – TTP (*Trusted Third Party*) za obezbeđivanje određenih svojstava razmene podataka.

9.2.5. Bezbednost bežičnih lokalnih mreža

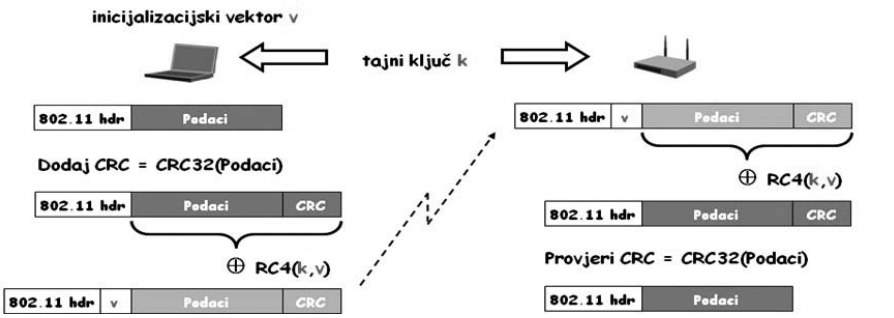
Svi tipovi *bežičnih lokalnih mreža* – **WLAN** (*Wireless LAN*) sa različitim brzinama prenosa imaju iste osnovne bezbednosne probleme – koriste radio frekvencije za prenos informacija, koje se lako mogu kompromitovati (Tabela 9.7).

Tabela 9.7. Standardni tipovi bežičnih mreža

Standard	Frekvencija	Osnovna/Realna propusna moć	Kompatabilnost sa 802.11b	Godina primene	Domet In/Out (m)
802.11a	5Ghz	54 /25 Mbps	Ne	2002	35/120
802.11b	2.4Ghz	11/5 Mbps	Da	1999	38/140
802.11g	2.4Ghz	54/1 Mbps	Da	2003	75/400
802.11i	2.4Ghz	54/1 Mbps	Da	2004	100/400
802.11e	2.4Ghz	144/35 Mbps (mobilni pristup)	Ne	2005	100/400
802.16n	5Ghz	600/288,9 Mbps (mobilni pristup)	Ne	2010	70/250

Bežični LAN (WLAN) je *Ethernet LAN* bez kablovske infrastrukture. Lako se implementira, štedi mrežnu infrastrukturu i ima najveću praktičnu primenu od svih bežičnih mreža. Bežična tehnologija je izgrađena na bazi IEEE 802.11b standarda u SAD [7, 14, 36, 57] i *GSM* (*Groupe Spécial Mobile*) standarda u EU. Prema WLAN standardu IEEE 802.11b, informacije se prenose sa WEP protokolom (*Wireless Equivalent Protocol*) za zaštitu *CIA* informacija, slično prenosu fizičkim putevima.

WEP protokol radi na fizičkom i sloju veze podataka OSI modela, a zasniva se na šifrovanju podataka između krajnjih tačaka. Međutim, od 2001. godine hakeri uspešno krekuju i modifikuju WEP poruke na WLAN mrežama na više načina, zbog ranjivosti **RC4** algoritma, koji se može probiti i omogućiti pristup mreži. *Standard zaštite 802.11* obezbeđuje *šifrovanje* i *autentifikaciju*. Prvi cilj zaštite 802.11 je otklanjanje detektovanih slabosti WEP protokola (Sl. 9.21).



Sl. 9.21. Funkcionalni model WEP protokola

Autentifikacija se vrši potprotokolom *ap4.0.* Host računar zahteva autentifikaciju od pristupne tačke (**AP**), koja šalje 128 bitni SN zahtev (R). Host šifruje R primenom simetričnog ključa, a AP dešifruje R i autentifikuje host. Dakle, ne postoji mehanizam za distribuciju ključa, a za autentifikaciju je dovoljno poznavati simetrični ključ. Za šifrovanje podataka WEP protokolom, host/AP dele 40-bitni simetrični, polutrajni ključ. Zatim host dodaje 24-bitni *inicijalizujući vektor* (**IV**) za kreiranje 64-bitnog ključa, koji se koristi za generisanje niza ključeva–ki**IV**, a ovi se koriste za šifrovanje i-tog bajta - di, u frejmu: **ci = di XOR** – **kiIV,** u kojem se **IV** i šifrovani bajtovi - ci, šalju zajedno.

Glavni bezbednosni propust WEP protokola je otvoreno i ponovljeno slanje 24–bitnog **IV** (jedan po frejmu). Ponovljeno korišćenje **IV,** napadač može detektovati i izazvati stanicu **A** da šifruje poznatu poruku d1 d2 d3 d4 …. Napadač vidi šifrat: ci = diXORki**IV**, a kako poznaje cidi, može izračunati ki**IV**. Napadač zna sekvence ključeva za šifrovanje k1**IV**k2**IV**k3**IV** i, ako se sledeći put upotrebi poznati **IV**, može uspešno da dešifruje poruku.

Napadači koji su pristupili WLAN mreži mogu veoma efektivno izvesti napade preko DNS servera, protiv svakog korisnika u mreži, jer mogu da vide DNS zahtev i lažno odgovore, pre nego sto DNS server stigne da odgovori na njega. Ozbiljan problem sa WLAN nije samo WEP protokol, nego i pristup mreži (prijem signala). Mnoge poslovne mreže instaliraju AP bez uključene zaštite, da bi se besplatno koristile. Za većinu AP, konfigurisanih bez šifrovanja, mogu se konfigurisati OS, kao što su Windows XP SP2 i MAC OS X, tako da se automatski priključe na svaku dostupnu bežičnu mrežu. Korisnik koji pokrene laptop u blizini AP, može da ustanovi da se računar povezao na mrežu bez ikakvog vidljivog nagoveštaja. Takođe, korisnik koji namerava da se poveže na jednu mrežu, može završiti u drugoj, ako ima jači signal. U kombinaciji sa automatskim nalaženjem uređaja druge mreže (npr. DHCP i *Zeroconf*), ovo bi moglo da navede bežičnog korisnika da pošalje osetljive identifikacione podatke pogrešnom provajderu i uloguje na *web* sajt kroz nesigurnu mrežu. WLAN mreže 802.11 u 85% slučajeva ne koriste mehanizme šifrovanja i autentifikacije pa su *pretnje za WLAN* brojne. Podložne su *packet–sniffing,* DoS i drugim vrstama napada. Na primer, mikrotalasna pećnica sa premošćenim mehanizmom za zatvaranje vrata, kada radi sa otvorenim vratima, stvara smetnju od 1000 W na istoj frekvenciji kao i uređaji standarda 802.11b.

Značajnije *bezbednosne pretnje* WLAN su da maliciozni korisnici mogu:

- dobiti nedozvoljen pristup internoj mreži kroz bežičnu mrežu,
- presresti osetljive ne-šifrovane informacije, koje se šalju kroz WLAN,
- ukrasti na mreži identitet legitimnog korisnika i zloupotrebiti ga,
- izvršiti DoS napad na bežičnu mrežu ili uređaj,
- kroz WLAN anonimno izvesti napad na druge mreže i
- postaviti lažnu AC i namamiti legitimne korisnike na lažnu AP.

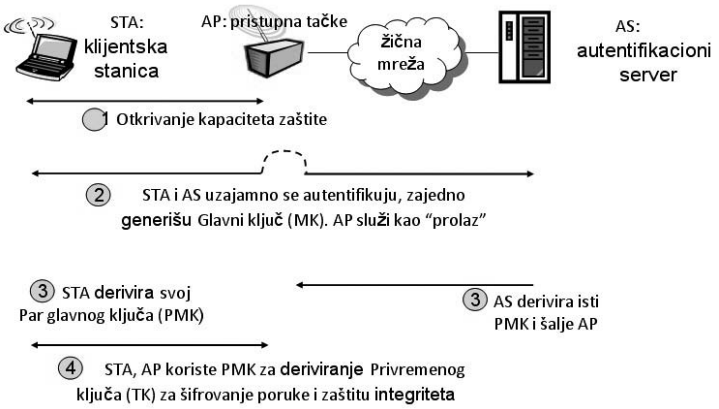
Faktori rizika WLAN 802.11 se mogu svrstati u sedam osnovnih kategorija: *ubacivanje u tok saobraćaja (Insertion Attacks), ometanje (Jamming), kriptoanalitički napad*

(Encryption Attacs), izviđanje i intercepcija saobraćaja (War Driving), kolaborativni rad mobilnih uređaja (prenos malicioznog kôda), rekonfiguracija sistema i napadi brutalnom silom. Svaki od navedenih faktora rizika WLAN sistema mogu se redukovati ili izbeći sa propisnim korišćenjem politike i najbolje prakse zaštite.

Mere zaštite od neovlaštenog pristupa uključuju WEP zaštitni protokol i potiskivanje emitovanja SSID pristupne tačke, čime se dopušta pristup samo računarima sa poznatim MAC adresama. Potiskivanje SSID i filtriranje MAC adresa su neefikasne metode zaštite, jer se SSID emituje otvoreno, kao odgovor na klijentski SSID upit, tako da MAC adresa lako može da se zloupotrebi. Ako napadač može da promeni svoju MAC adresu, može i da se spoji na mrežu zloupotrebom ovlašćenih adresa. WEP šifrovanje pruža zaštitu od povremenih upada, ali zbog ranjivosti RC4 algoritma, neki dostupni alati, kao što su *AirSnort* ili *AirCrack–ptw*, mogu otkriti WEP šifrovane ključeve. *AirSnort* može da otvori šifru za manje od sekunde, jer vidi oko 5–10 miliona šifrovanih paketa. Noviji alat, *AirCrack–ptw,* koristi *Klajnov* napad za razbijanje WEP ključa, sa uspehom od 50%, upotrebom samo 40.000 paketa.

WPA (*WiFi Protected Access*) sistem zaštićenog pristupa WLAN mreži je poboljšan protokol zaštite, dizajniran je da zameni manje bezbedan WEP protokol u 802.11i mreži. Uključuje mogućnost šifrovanja podataka i autentifikacije korisnika. Podaci se šifruju RC4 algoritmom sa 128–bitnim ključem i 48–bitnim inicijalizacijskim vektorom. Prednost nad WEP protokolom je u korišćenju **TKIP** protokola (*Temporal Key Integrity Protocol*), koji dinamički menja ključeve u toku rada sistema. Kombinacijom dugačkog **IV** i **TKIP** protokola sistem postaje otporniji na napade, koji su rizični za WEP protokol, ali već ima poznat vektor napada.

WPA 2 (*WiFi Protected Access 2*), sličan WPA protokolu**,** koristi napredn**i** AES–CCMP algoritam ***(****Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol***)** i obezbeđuje znatno veći nivo zaštite u 802.11i mreži. Princip rada standarda 802.11i prikazan je na Sl. 9.22.



Sl. 9.22. Princip rada 802.11i u četiri faze

WPA 2 rešava većinu ozbiljnih ranjivosti WEP šifarskog sistema, obezbeđuje distribuciju ključeva i koristi autentifikacioni server, nezavisno od AP [71]. **WEPplus** ima veću efikasnost, onemogućavanjem korišćenja loše oblikovanih IV. Uporedne vrednosti bezbednosnih funkcija glavnih protokola zaštite u WLAN sistemima date su u Tabeli 9.8.

Tabela 9.8. Uporedne vrednosti funkcija protokola zaštite WLAN sistema

	IEEE 802.11b WEP	WPA	IEEE 802.11i (WPA2)
Tajnost podataka (enkripcija)	WEP (RC4)	TKIP (RC4)	AES, (opcija TKIP)
Integritet podataka	WEP (RC4) + CRC	TKIP-MIC	AES-MAC (opcija TKIP-MIC)
Autentikacija i kontrola pristupa	Shared Key Authentication	IEEE 802.1X/EAP (+ EAP-TLS, LEAP…)	IEEE 802.1X/EAP (+ EAP-TLS, LEAP…)

LEAP (*Lightweight Extensible Authentication Protocol*) protokol za autentifikaciju, baziran na 802.1x standardu, dizajniran je da smanji ranjivost WEP–a primenom sofisticiranog vođenja sistema ključeva. LEAP ili *Dynamic WEP* dinamički menja WEP ključeve. Dinamički generisani ključevi i međusobna autentifikacija između klijenta i RADIUS servera, omogućavaju da se klijenti često ponovo autentifikuju, a tokom uspešne autentifikacije dobijaju novi WEP ključ. Stalnim generisanjem novih ključeva i kratkim trajanjem svakog pojedinačno, povećava se zaštita ključa od otkrivanja hakerskim napadom. Ipak, dostupni alati tipa *THC–LeapCracker*-a omogućavaju probijanje LEAP zaštite i napad rečnikom na klijenta.

PEAP (*Protected Extensible Authentication Protocol*) protokol su razvili *Cisco, Microsoft* i *RSA Security*. PEAP (čita se "**pip**") nije kriptološki protokol i služi samo za autentifikaciju klijenta u mreži. Koristi DS na serverskoj strani za autentifikaciju klijenta, kreiranjem SSL/TLS tunela između klijenta i autentifikacijskog servera i na taj način štiti podatke, koji se prenose mrežom.

RADIUS *(*Remote Authentication Dial In User Service*) servis predstavlja odličnu zaštitu od napada hakera. Spada u AAA (Authentication, Authorization & Accounting) protokole, što znači da obezbeđuje autentifikaciju, autorizaciju i upravljanje korisničkim nalogom. Ideja korišćenje servera unutar sistema, koji verifikuje korisnike preko korisničkog imena i korisnički izabrane lozinke. Pomoću RADIUS servera korisnicima se mogu dodeljivati razne dozvole i ograničenja, npr. za potrebe naplaćivanja usluge korišćenja. Negativna strana ovakvog sistema je u investiranju u server koji će obavljati RADIUS funkciju.*

GSM – *Evropski sistemi mobilne telefonije* ima brojne ranjivosti **–** SIM kartice, SMS servisa, GPRS servisa i WAP protokola [57].

Treća generacija (3–G) tehnologije bežičnih sistema, usmerena na poboljšanje komunikacije podataka i glasa bežičnim putem, koriguje sve uočene bezbednosne ranjivosti

navedenih standarda. Neposredni cilj je povećanje brzine prenosa na 2 Mb/s i frekvencije prenosa na 5,1 GHz. Cilj je razviti skalabilan sistem, koji se može nadograditi sa poboljšanim kontrolama zaštite, kada je potrebno. Identifikovani tipove napada na WLAN mreže, na frekvencijama od 2 GHz i 2,5 GHz, u 3–G WLAN mreži su eliminisani. *Sistem zaštite 3–G WLAN* zasniva se na zaštiti GSM standarda sa sledećim važnim izmenama:

- onemogućen napad na baznu stanicu sa lažnim predstavljanjem,
- veća dužina WEP ključa i dopušta implementaciju jačeg algoritma (AES),
- uključeni mehanizmi zaštite unutar i između WLAN mreža,
- mehanizmi zaštite su u svičerima i štite vezu do bazne stanice,
- integrišu se mehanizmi za zaštitu integriteta i autentifikaciju terminala,
- dato je uputstvo za izbor drugog autentifikacionog algoritma i
- u *roming* vezi između mreža, aplicirana je zaštita smart karticom.

Sistem zaštite *3–G WLAN* je znatno bolji od zaštite GSM, ali se mogući napadi ne mogu potceniti. Potencijalne slabosti *3–G WLAN* mreža mogu biti *logovanje na lažnoj baznoj stanici i forsiranje komunikacije bez kriptozaštite*.

Na osnovu kriterijuma za vrednovanje kriptoloških algoritama, mogu se izvući sledeći zaključci za praktičnu primenu kriptoloških mehanizama u zaštiti RM:

1. simetrični kriptografski algoritam sa tajnim ključem treba koristiti za zaštitu informacija u bežičnim i mobilnim mrežama i na komunikacijama,
2. za generisanje i razmenu ključeva treba koristiti asimetrični algoritam,
3. za integrisane kriptološke mehanizme najbolji metod je kombinovana simetrična i asimetrična kriptografija,
4. asimetričnu kriptografiju koristiti za identifikaciju i autentifikaciju,
5. podatke od korisnika do bazne stanice štititi simetričnim algoritmom,
6. mehanizam zaštite je bolje realizovati u baznim stanicama, jer je lakše održavati njihov integritet, nego štititi protokol pristupa tim stanicama,
7. za svaku logičku vezu koja traži zaštitu podataka, treba generisati novi kriptografski ključ,
8. kontrolne parametre treba štititi prema zahtevima 4 i 5.

9.3. REZIME

Servis *kontrole pristupa RM–i* vrše mrežne barijere, koje nameću politiku kontrole pristupa između dve ili više segmenata RM i obezbeđuju mrežnu zaštitu po dubini. Postoje dve značajne klase barijera, koje rade na principu kontrole *stanja* veze i filtriranja rutiranih IP paketa, a mogu se implementirati na mrežnom sloju sa rutiranjem paketa i aplikativnom sloju ili kao *proksi* barijere, koje ne rutiraju direktno pakete. Proksi serveri posreduju između nepoverljive i poverljive RM i kontrolišu konekcije koje dolaze iz RM.

Najčešći su u praksi *web proksi serveri*.

Autentifikacioni uređaji – smart kartica, biometrijski uređaj, token za bezbedno skladištenje kriptografskih informacija ili *token* kao priručni uređaj, koriste se za autentifikaciju. Za visoku bezbednost IKTS i zaštitu kriptografskih tajni, koriste se smart kartice na korisničkoj i HSM kriptografski moduli na serverskoj strani. *Kriptografski akceleratori* kombinuju sigurno skladištenje ključeva, kriptografiju visokih performansi i veću skalabilnost kriptografskih aplikacija.

U RM, podaci se prenose u otvorenoj formi preko TCP/IP protokola i mogu se lako prisluškivati. Za zaštitu pristupa koriste se autentifikacioni protokoli tipa SSL – za zaštićen prenos lozinke i *Kerberos* tipa, koji rade na principu upita – odgovora. Za centralizaciju procesa autentifikacije i autorizacije prava pristupa autentifikovanih entiteta u RM, koriste se *A&A serveri*. RADIUS ili TACACS + protokoli uobičajeno se koriste za kontrolu udaljenog pristupa.

Monitoring i integritet intraneta obezbeđuju NIDPS, skeneri saobraćaja i kapaciteti za upravljanje incidentom i oporavak sistema. Zaštita integriteta u mrežnom okruženju zahteva zaštitu integriteta podataka i komunikacione sesije. NIDPS, u većini slučajeva, rade na mrežnom sloju, detektuju sisteme nezavisno od OS i omogućavaju zaštitu brojnih platformi. NIDPS i mrežni skeneri rade na istim principima kao HIDPS i skeneri RS, s tim da otkrivaju ranjivosti RM. Skeneri telefonskih veza, koriste se za identifikovanje potencijalnih ranjivosti sistema preko telefonske linije.

Kriptografski mehanizmi i protokoli zaštite izvršavaju i integrišu mrežne servise zaštite *poverljivosti, integriteta i neporecivost, digitalnog potpisa i jake autentifikacije* kroz PKI sistem. Osnovni moduli PKI sistema su CA, RA i Imenik. Postoje hijerarhijska, rešetkasta, hibridna i tranzitivna organizaciona struktura arhitekture PKI sistema.

Zaštita poverljivosti mrežnih podataka vrši se šifrovanjem – asimetričnom PKI kriptografijom za razmenu simetričnog ključa i simetričnom – za šifrovanje podataka na prenosnom putu. Asimetrična PKI kriptografija otvoreno distribuira *javni ključ (Pk),* matematički uparen sa jedinstvenim *privatnim ključem (Tk)*. PKI obezbeđuje okvir za protokole zaštite transakcija. Primeri su SSL, TLS i IPsec protokol, koji je najpoželjniji za implementaciju VPN.

Bežična lokalna mreža (*WLAN)* se lako implementira i obezbeđuje veliku uštedu komunikacione infrastrukture. Tehnologija *WLAN* je izgrađena na bazi *IEEE 802.11b* standarda u SAD i *GSM* standarda u EU. *WEP* (*Wireless Equivalent Protocol*) protokol za zaštitu prenosa, dizajniran za zaštitu *CIA* informacija na prenosnom putu, pokazao je brojne slabosti *RC4* algoritma. Poboljšanu zaštitu obezbeđuju WPA i WPA(2), *WEPplus i Dynamic* WEP (tekući standard *802.11i*).

Treća generacija tehnologije WLAN koriguje sve uočene bezbednosne ranjivosti WEP protokola i poboljšava komunikaciju podataka i glasa bežičnim putem, koristeći bilo koji od raspoloživih standarda.

9.4. KLJUČNI TERMINI

Autentifikacioni protokoli*:* standardno su ugrađeni u sam proces razmene podataka; koriste dodatne mere zaštite poverljivosti, integriteta i neporecivosti.

Autentifikacioni serveri: centralizuju procese autentifikacije u RM.

Autentifikacioni uređaji: obezbeđuju korisniku neki fizički identifikator za kompletiranje autentifikacije (*smart* karticu, biometrijski uređaj i token).

Autorizacioni serveri: pridružuju skup privilegija pristupa autentifikovanim entitetima.

Biometrijski uređaji: verifikuju identitet korisnika na bazi jedinstvenih, fizičkih atributa (otisak prsta, dlana, mrežnjače oka itd.).

Hardversko–softverski modul – HSM (*Hardware Storage Module/H Software M*): koristi se na serverskoj strani za skladištenje kriptografskih tajni.

Infrastruktura sa javnim ključem–PKI (*Public Key Infrastructure)*: asimetrična kriptografija sa parom javnog i privatnog ključa; glavni moduli su CA, RA Imenik.

Kriptografski akceleratori: Specijalizovani HSM, koji kombinuju bezbedno skladištenje ključeva, kriptografiju visokih performansi i skalabilnost aplikacija.

Kriptografski protokoli: štite podatke na prenosnom putu, implementiraju i izvršavaju servisa zaštite autentifikacije, poverljivosti, integriteta i neporecivosti.

Proksi server: slično *gateway* barijeri kontroliše i posreduje veze koje dolaze izvan i iz RM.

Server mrežnog pristupa – NAS (*Network Access Server*): dopušta konekciju sa PSTN na zahtevani interni host, nakon autentifikacije i primene neke restrikcije.

Skeneri telefonskih veza: identifikuju ranjivosti sistema preko telefonske linije.

Skeneri zaštite RM: slični su skenerima zaštite RS, s tim da otkrivaju ranjivosti RM.

Smart kartice: autentifikacioni uređaj sa čitačem; *memorijske* za skladištenje ili *mikroprocesorske* za skladištenje ključeva i kriptografske operacije na samoj kartici.

Tokeni: autentifikacioni uređaji za bezbedno skladištenje kriptografskih informacija.

9.5. PITANJA ZA PONAVLJANJE

1. Metod sistema jake autentifikacije za pristup administrativnim nalozima RM je:
   a. korisnički nalog i lozinka
   b. kriptografska smart kartica sa PIN–om
   c. biometrijski uređaj ili token
2. Koji se bezbednosni kvalitet dobija upotrebom NIDS sistema:
   a. detektuju upade nezavisno od OS i omogućavaju zaštitu više platformi
   b. vidi napade sa Interneta koji probijaju odbranu spoljnog perimetra RM
   c. ne ističu probleme sa politikom ili funkcionisanjem mrežne *barijere*
   d. ne vidi napade na *web* ili *FTP* server, koji su obično smešteni u DMZ
   e. dokumentuje tipove i broj napada koji potiču sa Interneta, a pogađaju RM
   f. monitoriše mrežni saobraćaj i povećava mogućnost detekcije napada
   g. detektuje ovlašćene aktivnosti legalnih korisnika iz RM organizacije

3. Neki problemi vezani za upotrebu NIDPS sistema su:
   a. ne mogu detektovati anomalije bez prepoznavanja protokola
   b. ne mogu interpretirati podatke
   c. mogu igrati važnu ulogu u upravljanju malicioznim kodovima
   d. ne mogu igrati važnu ulogu u upravljanju malicioznim kodovima
   e. mogu biti konfigurisani da sprečavaju prolaz inficiranih objekata izvan intraneta
4. *Autentifikacioni* i *autorizacioni* serveri u sistemu mrežne zaštite:
   a. koriste se za decentralizovano upravljanje procesom autentifikacije u RM
   b. obuhvataju skup privilegija ili prava pristupa entiteta korisnika
   c. obavezni su u sistemima za kontrolu pristupa sa udaljenih mrežnih lokacija
   d. obezbeđuju servise za više klijenata u klijent–server arhitekturi
   e. mogu dodeljivati uloge korisnicima
   f. ne povećavaju značajno bezbednost pristupa udaljenih korisnika
   g. ne štite podatke koji se izmenjuju između korisnika i internog sistema
5. Ključni moduli tipičnih skenera ranjivosti RM su:
   a. modul za skeniranje,
   b. baza podataka sa poznatim ranjivostima (definicijama mrežnih napada)
   c. modul za generisanje i prezentaciju izveštaja
   d. modul korisničkih interfejsa
   e. modul za identifikaciju malicioznih programa
6. Glavni alat za kontrolu pristupa RM je:
   a. korisnički nalog i lozinka
   b. logička barijera (*firewall*)
   c. NIDPS,
   d. web filteri i proksi serveri
7. Proksi serveri su:
   a. namenjeni uglavnom za kontrolu konekcija koje dolaze iz interne RM
   b. namenjeni uglavnom za kontrolu konekcija koje dolaze sa Interneta
   c. ne zahtevaju autentifikaciju krajnjeg korisnika
   d. ograničavaju dopuštene komunikacije na definisani skup protokola
   e. primenjuju restrikciju kontrola pristupa i loguju kontrolne tragove
   f. najčešći tip u praksi su *web proksi serveri*, koji se koriste samo za zaštitu
   g. višefunkcionalni alati koji ne implementiraju značajnu zaštitu
8. Servis zaštita integriteta u mrežnom okruženju obuhvata:
   a. integritet podataka
   b. integritet sesije komunikacije
   c. integritet sinhronizacije protokola
   D. ni jedan gore naveden
9. Glavni nedostatak PKI sistema je:
   a. poverenje korisnika u povezanost javnog ključa i nominalnog vlasnika
   b. poverenje u digitalni sertifikat, koji izdaje CA
   c. ne garantuje povezanost javnog ključa (Pk) sa imenom vlasnika na poverljiv i bezbedan način
   d. ni jedan gore naveden
10. Osnovni standard za bežične mreže WLAN (*IEEE 802.11b)* ima implementiran:
    a. WEP (*Wireless Equivalent Protocol*) protokol za zaštitu
    b. WAP (*Wireless Application Protocol*) protokol
    c. WAP (2)
    d. ICMP protokol
11. Višeslojna antivirusna zaštita vrši se:
    a. za proveru autentičnosti, zaštitu integriteta i neporecivosti
    b. za generisanje digitalnog potpisa i bezbedno čuvanje kriptografskih tajni
    c. za otežavanje primene metoda kriptoanalize
    d. na kapiji, ruteru, serveru mreže i radnim stanicama
12. Izolacija RM vrši se:
    a. obezbeđivanjem jednoznačnih identifikacionih parametara
    b. radi zaštite od DoS/DDoS napada

c. sa mrežnim kapijama za filtriranje paketa
d. radi sprečavanja unošenja aktivnih malicioznih programa

13. Kriptološki mehanizmi zaštite u RM koriste se za:
    a. proveru autentičnosti, zaštitu integriteta, poverljivosti i neporecivosti
    b. generisanje digitalnog potpisa i bezbedno čuvanje kriptografskih parametara
    c. za otežavanje primene metoda kriptoanalize
    d. za zaštitu tajnosti podataka i lozinki
14. Tehnologija digitalnog potpisa se koristi za:
    a. proveru autentičnosti, zaštitu integriteta i neporecivosti
    b. generisanje digitalnog potpisa i bezbedno čuvanje kriptografskih parametara
    c. otežavanje primene metoda kriptoanalize
    d. bezbednu autentifikaciju strana u komunikaciji
15. Za zaštitu poverljivosti informacija u RM koriste se dve osnovne tehnika:
    a. obezbeđivanje jednoznačnih identifikatora i razmena sesijskog ključa
    b. upotreba protokola za uspostavljanje ključa i generisanje simetričnog ključa
    c. generisanje simetričnog ključa, šifrovanje sa javnim ključem (Pk) udaljenog korisnika i transfer sa asimetričnim PKI sistemom
    d. bezbedna autentifikaciju strana u komunikaciji i razmena simetričnog ključa
16. Digitalni sertifikat se koristi za:
    a. proveru autentičnosti, zaštitu integriteta i neporecivosti
    b. generisanje digitalnog potpisa i bezbedno čuvanje kriptografskih tajni
    c. sprečavanje primene metoda kriptoanalize
    d. višeslojnu zaštitu na kapiji, ruteru, serveru mreže i radnim stanicama
17. *Smart* kartica se koristi za:
    a. proveru autentičnosti, zaštitu integriteta i neporecivosti
    b. generisanje digitalnog potpisa i bezbedno čuvanje kriptografskih tajni
    c. za otežavanje primene metoda kriptoanalize
    d. zaštitu na kapiji, ruteru, serveru mreže i radnim stanicama
18. Kriterijumi za izbor biometrijskih parametara mogu biti:
    a. performanse, pouzdanost i pogodnost za primenu
    b. kompleksnost sistema zaštite i troškovi nabavke
    c. sposobnosti korisnika i korisnička prihvatljivost
    d. troškovi obuke korisnika
19. Ograničenja PKI za veliki broj korisnika prevazilazi:
    a. *AutoGuard* uređaj i SNTP protokol (US patent)
    b. *ProGurad* uređaj i MEDIJA protokol (US patent)
    c. *AutoGuard* uređaj i MEDIA protokol (US patent)
    d. *AutoGuard* uređaj i MSNG protokol (US patent)
20. Za šifrovanje VPN veze najčešće se koristi:
    a. SSL protokol
    b. HTTPS protokol
    c. IPSec protokol
    d. TTPS protokol

9.6. LITERATURA

[1] American Bar Association, Section of Science &Technology Law, Privacy & Computer Crime Committee, *International Strategy for Cyberspace Security*, *www.abanet.org/abapubs/books/cybercrime/*, 2003.

[2] Bace, R., Mell, P., *Intrusion Detection Systems,* NIST SP 800–31, http://www.csrc.nist.gov/publications, 2006.

[3] Barker, W. C.**,** *Guide for Mapping Types of Information and Information Systems to Security Categories,* NIST SP800–60 –1 i 2, http://www.csrc.nist.gov/publications, juni 2004.

[4] Bjork, Fredrik, *Security Scandinavian Style–Interpreting the practice of managing information security in organisations*, Stockholm University, Rozal Institute of Technology, 2001.

[5] Bruce, S., *Applied Cryptography: Protocols Algorithms and Source Code in Cryptography*, 2nd edition, New York, John Wiley and Sons, 1996.

[6] BSI (Federalni IS Nemačke), *IT Baseline Protection Manual***,** *http://www.bsi.bund. de/gshb*, juli 2005.

[7] Burns, J. *Evolution of WLAN Security*, http://www.mtghouse.com/MDC_ Evolving_Standards.pdf, 2004.

[8] Cambra, R., *Metrics for Operational Security Control*, Sans Institute, 2004

[9] Carrel, D., i Grant, L., *The TACAS+ Protocol,* http://casl.csa.iisc.ernet.in/ Standards/ internet–drafts/draft–grant–tacas–02.txt, 2003.

[10] Carrol, M.J., *Computer Security*, Butterworth–Heinemann, 1997.

[11] Castell, B. S., Gray G., Muller P., *User Requirements for Trusted Third Party Services*, INFOSEC Project Report S2101/01, Commission of the European Communities, DG XIII, B–6, Oct 1993.

[12] CCIMB–99–031, *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, Version 2.1, http://www.commoncriteria. org, 1999.

[13] CERT*, http://www.cert.org/advisories*, 2003.

[14] Christopher, W.K.s, *Wireless LAN Security FAQ*, http://www.iss.net/ wireless/ WLAN_FAQ.php, 2003.

[15] Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., i Graffo, L., *Performance Measurement Guide for Information Security*, NIST Special Publication SP800–55–rev1, July 2008. http://csrc.nist.gov/ publications/PubsSPs.html

[16] COAST (*Computer Operations, Audit, and Security Technology*), Pardu univerzitet, SAD, http://www.cs.purdue.edu/ coast/#archive, 2003.

[17] COBIT (*Control Objectives for Information and Related Technologies*), http:// www.isaca.org, 2009.

[18] CRAMM, http://*www.crammusergroup.org.uk*, 2008.

[19] Curtin, M., Ranum, M.J., *Internet Firewalls: FAQ,* http://www.interhack.net/ pubs/fwfaq., 2003.

[20] Debra, S. Herrmann, *Complete guide to security and privacy metrics: Measuring Regulatory Compliance, Operational Resilience and ROI*, Auerbach Publications Taylor & Francis Group, LLC, 2007.

[21] Domarev, V., *Защита информации и безопасность компьютерных систем*, http://www.security.ukrnet.net/, 1997.

[22] Drake, D. L. i Morse K. L., *The Security – Specific Eight Stage Risk Assessment Methodology*, Proceedings of the 17th NCSC, Baltimore, October 1994.

[23] ElcomSoft, istraživanje, 2009.

[24] Ferrari, J. i dr., *Smart Cards: A Case Study,* http://www.redbooks.ibm.com/ redbooks/pdfs/sg245239.pdf, avgust 2003.

[25] FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, http://www.itl.nist.gov/l/fipspubs, juni 2005.

[26] Frankel, S*., An Introduction to IPsec*, http://www.csrc.nist.gov/ buliten, 2001.

[27] GAISP*, Generally Accepted Information Security Principles*, http://www.gaisp.org, 2009.

[29] Gerencser M., Aguirre, D., *Security Concerns Prominent on CEO Agenda, Strategy+Business Press*, http://www.strategy–business.com/press/ enewsarticle/22197, 2002.

[30] Kovacich, G. L., i Halibozek, E. P., *Security metrics management: how to measure the costs and benefits of security*, 2006.

[31] Grance, T., Hash, J., Stevens, M., O'Neal, K., *Bartol, N., Guide to Information Technology Security Services*, NIST SP 800–35, http://csrc.nist.gov/publications/ nistpubs/800–35/sp800–35.pdf, 2003.

[32] Grance, T., Hash J., Stevens M., *Security Considerations in the Information System Development Life Cycle*, NIST SP 800–64, http://csrc.nist.gov/publications/ nistpubs/800–64/sp800–64.pdf, juni 2004.

[33] Grance, T., Kent K., Kim B., *Computer Security Incident Handling Guide*, NIST SP 800–61, http://www.nist.gov/publications, January 2004.

[34] Grubor, Gojko, *Katalog kontrola sistema osnovne zaštite za nizak uticaj pretnji*, skripta, Univerzitet SINGIDUNUM, FPI, maj 2006.

[35] Grubor, Gojko, *Razvoj i upravljanje programom zaštite zasnovanim na modelu sazrevanja procesa,* doktorska disertacija, Univerzitet Singidunum, 2007.

[36] Harold, F. T., Micki K., *The information security handbook*, http://csrc.nist.gov/policies/ombencryption–guidance.pdf, 2003.

[37] Heyer, J., *WLAN Security: Wide Open*, http://www.tomsnetworking.com/network/20020719/index.html, 2004.

[38] Housley, R. i dr., *Internet X509 Public Key Infrastructure: Certificate and CRLProfile (RFC 2459),* http://www.ietf.org/rfc/rfc2459.txt., 2007.

[39] Howard, D. J., *An analizis of Security Incedent 1989/1995,* Doctor's Thesis, Carnegie Mellon University. 1997.

[40] IETF, *Policy Framework*, http://*www.ietf.org*, 2005.

[41] Information Security Forum (ISF), *Information Security Metrics – Report*, May 2006, http://www.securityforum.org/

[42] IBM, *Proventia Desktop Endpoint Security*, http://www.ibm.com/services/iss, 2010.

[43] ISACA, *Information Systems Audit and Control Association*, http://www.isaca.org, 2003.

[44] ISF, *The Standard for Good Practice for Information Security*, http://www.isf.org, V.4.0., 2007.

[45] ISO/IEC 13335, *Gudelines for the management of IT Security*, http://www.iso.13335.org, 2003.

[46] ISO/IEC 15408, *Common Criteria/ITSEC*, http://www.iso.15408.org, 2003.

[47] ISO/IEC15443, *Information Technology– Security Techniques*, http://www.iso.15443.org, 2000.

[48] ISO/IEC 15504 (CMM), http://www.iso.15504.org, 2008.

[49] ISO/IEC 17799:2000, *Information Technology – Code of practice for information security management*, http://www.iso.org, 2003.

[50] ISO/IEC 21827 (SSE CMM*), System Security Engeneering Capability Maturity Model,* http://www.iso.21827.org., 2003.

[51] ISO/IEC 27001, *Information Security Management System*, http://www.iso.27001.org, 2008.

[52] ISO/IEC 27005, **http://www. iso.27005.org**, 2008.

[53] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement* (draft). http://www.iso.org/iso/

[54] ISS, *Dynamic Threat Protection™: A New Definition for Information Security*, http://www.iss.org, 2005.

[55] ITU–T, *Information Technology – Open system Interconnection – The directory: Public key and attribute certificate frameworks*, Recommendation X.509, 2007.

[56] ITU–T, *Information Technology – Open system Interconnection – The directory: overview of concepts, models and services*, Recommendation X.500, 2007.

[57] Jaquith, A., *Security Metrics: Replacing*

Fear, Uncertainty, and Doubt, Pearson Education, Inc., http://www.securitymetrics.org/content/Wiki.jsp, March 2007.

[58] Karygiannis, T., Owens, L., *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, NIST SP 800–48, http://www.csrc.nist.gov/publications, 2008.

[59] Kelm, S., *The PKI page*, http://www.pki–page.org, 2008.

[60] Lee, A., Brewer, T., *Information security within the system development life cycle*, Jones Computer Security Division Information Technology Laboratory NIST, *http://www.itl.nist.gov/*, 2006.

[61] Manzuik S., Pfeil K., *Network Security Assessment–from vunerability to patch, Syngress,* 2007

[62] Milosavljević, Milan, Grubor Gojko, *Osnovi bezbednosti i zaštite informacionih sistema*, Univerzitet Singidunum, 2006.

[63] NIST – NSA Informal Note, *A Survey of Access Control Methods*, 2009.

[64] NIST SP 800–12*, An introduction to computer Security*, http://csrc.nist.gov/ publications/nistpubs/800–12/sp800–12.pdf, avgust 2003.

[65] NIST SP 800–14, *Genaerally Accepted Principles and Practices for Security*, http://csrc.nist.gov/publications/nistpubs/800–14/sp800–14.pdf, 2002.

[66] NIST SP 800–18, *Guide for developing Security Plans for IT Systems*, http://csrc.nist. gov/publications/nistpubs/800–18/sp800–18.pdf, 2003.

[67] NIST, *Trusted Security Evaluation Criteria*, http://www.radium.ncsc.mil/tpep, 1999.

[68] NIST SP 800–140–2, *Security Requirements for Cryptographic Modules*, 25.05 2001., http://csrc.nist.gov/publications/fips/fips140–2/fips1402.pdf.

[69] *OCTAVE® methods and criteria*, http:// www.cert.org/octave, 2005.

[70] *OCTAVE®method Implementation Guide*, http://www.cert.org/octave/osig.html, 2005.

[71] Opacki, D.,CISSP, *Security Metrics: Building Business Unit Scorecards*, dopacki@ covestic.com, December 2005.

[72] Ou G., *Understanding the updated WAP and WAP2 standards*, http://blogs.zdnet.com/Ou/?p=67, 2002

[73] Ozier, W., *Risk Analysis and Assessment, Handbook of Informaton Security Management*, CRC Press, Boca Raton, Florida, 1999.

[74] Partida, A., Andina, D., *IT Security Management: IT Securiteers – Setting up an IT Security Function*, Springer Science+Business Media, www.springer.com/ series/ 7818, 2010.

[75] Purser, S., *A practical guide to managing information security*, Artech House, Boston, London, 2005.

[76] Republika Srbija, *Predlog krivičnog zakona, Glava 27. „Krivična dela protiv bezbednosti računarskih podataka"*, član 298–304, 2004.

[77] Republika Srbija, *Zakon o borbi protiv visoko tehnološkog (kompjuterskog) kriminala*, Beograd, 2005.

[78] Republika Srbija, *Zakon o elektronskom potpisu*, revizija, Beograd, 2008.

[79] RFC 1320 i RFC 1321, http://www.icann.rfceditorc.org, 1997.

[80] RFC 2196, *Site Security Handbook*, http://www.ietf.org/rfc/rfc2196.txt, 1997

[81] Rigney, C., i dr., *Remote Authentication Dial In User Service (RADIUS),* RFC2138, http://www.faqs.org/rfc/rfc2138.html, 2003.

[82] Rodić, Boško, Đorđević, Goran, *Da li ste sigurni da ste bezbedni*, Produktivnost AD, Beograd, 2004.

[83] Ross, R., Swanson, M., &all, *Guide for the Security Certification and Accreditation of Federal Information Systems,* NIST SP 800–37, http://www.csrc.nist.gov/publications, 2004.

[84] Ross, R., Katzke, S., *Recommended Security Controles for Federal IS,* NIST SP 800– 53, A, B, C, http://www.csrc.nist.gov/publications, 2009.

[85] Russel, D., Gangemi, G.T. sr, *Computer Security Basics*, O'Reilly and Ass., 1995.

[86] Ruth, A., Hudson, K., *Sertificat Security +, MicrosoftCo.*, CET Beograd, 2004.

[87] SEI Institut, CMMI, www.sei.com. 2007.

[88] Scarfone, K., Mell, P., *Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST SP – 94, http://csrc.nist.gov/publications, 2007.

[89] Shirley, C. Payne, *A Guide to Security Metrics*, SANS Institute, InfoSec Reading Room, June 19, 2006. http://www.sans.org/reading_room/whitepapers/auditing/

[90] Snyder, J., *IDS and IPS*, Information Security magazine, maj 2009.

[91] Spears, J., Barton, R., Hery, W., *An Analysis of How ISO 17799 and SSE–CMM Relate to the S–vector Methodology*, http://www.ebrc.psu.edu, August 2004.

[92] Stoneburner, G., & all, *Risk Management Guide for Information Technology Systems*, SP 800–30, http://csrc.nist.gov/publications, 2002.

[93] Stoneburner, G., *Underlying Technical Models for Information Technology Security*, NIST SP 800–33, http://csrc.nist.gov/publications/nistpubs/800–33/sp800–33.pdf, decembar 2006.

[94] Stremus, P., *ISS IDC Security*, IDC simpozijum, pstremus@iss.net, Beograd 2006.

[95] Stallings W., *Network Security Essentials_ Applications and Standards*, 3rd Edition, Prentice Hall, USA, 2007.

[96] Swanson, M., Bartol, N., Sabato, J., Hash, J., i Graffo, L.*., Security Metrics Guide for Information Technology Systems*, NIST Special Publication 800–55, July 2009.

[97] The Help Net Security News, McAfee ***report***, 12.08.2010.

[98] Vaughn, R. B., Jr, *A practical approach to sufficient INFOSEC*, Mississippi State University, Department of Computer Science, *vaughn@cs.msstate.edu*, 2002.

INTERNET IZVORI:

http://www.isecom.org/projects/osstmm.htm,

http://www.atstake.com, 2006.

http://www.cert.org/incident_notes/index.html.

http://www.cert.org/tech_tips/security_tools.html#D.

www.sophos.com/pressoffice/news/articles/2008/03/lee–shin–ja.html (Posećeno: 20.04.2009.).

http://www.helpnet.securitynews.com, Panda lab izveštaj 2009. (Posećeno: 10.06.2010.).

http://www.helpnet.securitynews.com, *McAfee, Symantec godišnji izveštaj za 2008*, (Posećeno: 20.04.2010.).

http://cyberinsecure.com/computer–worm–infects–international–space–station–laptops/ (Posećeno: 20.04.2009.).

http://www.crn.com/security/56700144 (Posećeno: 20.04.2009.).

http://www.itl.nist.gov/fipspubs/fip180–1.htm.

http://www.physorg.com/news150486206.html *'Cybergeddon' fear stalks US: FBI*, (Posećeno: 20.04.2009.)

http://www.helpnet.securitynews.com, (Posećeno: 20.04.2009.).

http://www.kaspersky.com, (Posećeno: 20.04.2009.)

http://www.computereconomics.com/article.cfm?id=1225 (Posećeno: 20.04.2009)

http://vil.nai.com/vil/content/v_100119.htm (Posećeno: 20.04.2009.)

http://www.reghardware.co.uk/2008/10/08/asus_eee_box_virus/ (Posećeno: 20.04.2009).

http://www.symantec.com/, *Symantec Internet Security Threat Report*, 2008.

http://www.sophos.com, *Security threat report: 2009*, (Posećeno: 20.04.2010).

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

Glava II

UPRAVLJANJE SISTEMOM ZAŠTITE INFORMACIJA



UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

1. UPRAVLJANJE ZAŠTITOM INFORMACIJA

Po završetku ovog poglavlja razumećete:

- Metodologiju (principe, odgovornost,.) upravljanja zaštitom
- Proces integralnog upravljanja IKTS i sistemom zaštite
- Upravljačke kontrole najbolje prakse zaštite (ISO/IEC 27002)
- Metrički sistem za evaluaciju upravljanja zaštitom
- Preporuke za upravljanje zaštitom (ISO/IEC 27001)
- Otvorene probleme u oblasti upravljanja zaštitom

1.1. UVOD

Sa porastom obima e-poslovanja i integracije sistema, rastu i značaj upravljanja zaštitom, kritičnost procesa zaštite i legalna odgovornost menadžera za zaštitu. Proces upravljanja zaštitom obuhvata *proceduralne* i *tehničke kontrole zaštite* u kojima je čovek faktor odlučivanja. Sistem upravljanja zaštitom informacija – **ISMS** (*Information Security Managament Systemt*) je definisan standardom ISO/IEC 27001. Osnovni upravljački mehanizam ISMS je *politika zaštite*. Klase upravljačkih kontrola zaštite opisane su u standardima najbolje prakse zaštite (ISO/IEC 27001: Anex A; NIST SP 800–53 A, B, C rev.). U procesima ISMS od posebnog značaja je određivanje uloga i odgovornosti za izvršavanje i kontrolu procesa zaštite.

Da je upravljanje zaštitom informacija suštinski identično upravljanju rizikom u IKTS, prilično je očigledno i intuitivno prihvatljivo, ali nije sasvim tačno. Naime, razvijene su brojne metode za upravljanje rizikom, dok se komparativno slabija pažnja posvećuje upravljanju procesima zaštite u IKTS. Posledica je, da menadžeri, i prosečni korisnici vide zaštitu kao tešku i komplikovanu oblast, sa nerazumljivom terminologijom. Upravljanje zaštitom RS/RM obezbeđeno je procedurama zaštite, ugrađenim u rutinske računarske i mrežne operacije za održavanje CIA informacija i servisa. Tehnike upravljanja sistemom zaštite su brojne i obuhvataju sve kategorije upravljanja: *manuelnog*, *poluautomatskog* i *automatskog*. U oblasti upravljanja zaštitom, brojni su otvoreni problemi i očekuje se dalji razvoj.

1.2. METODOLOŠKI OKVIR ZA UPRAVLJANJE ZAŠTITOM

1.2.1. Principi upravljanja zaštitom

Opšte prihvaćeni principi zaštite (*GAISP*) čine bazu razvoja procesa za upravljanje zaštitom. Kako je proces za upravljanje rizikom najbliža aproksimacija procesa za upravljanje zaštitom, mogu se koristiti i generički principi za upravljanje rizikom, koji se implementiraju sa ukupno 16 *osnovnih aktivnosti* (Tabela 1.1).

Tabela 1.1. Glavni principi upravljanja rizikom

Principi UR	Osnovne aktivnosti
Procena rizika i određivanje potreba	Identifikovanje vrednosti informacione imovine
	Razvoj procedure za procenu rizika za poslovne procese
	Određivanje odgovornosti
	Neprekidno upravljanje rizikom
Uspostavljanje organizacije za centralno upravljanje rizikom	Određivanje radnog tima za upravljanje zaštitom
	Obezbeđivanje brzog pristupa tima glavnim izvršiocima odluka
	Obezbeđivanje potrebnog osoblja i drugih resursa
	Unapređivanje tehničke obuke i profesionalnosti tima
Implementacija politike i rentabilnih kontrola zaštite	Povezivanje politike zaštite sa faktorima rizika
	Definisanje razlika između politike i smernica (*guidelines*)
	Podržavanje politike kroz rad tima za upravljanje rizikom
Razvoj svesti i obuka o zaštiti	Neprekidna obuka korisnika o uticaju rizika i politike zaštite
	Upotreba tehnika zaštite prikladnih za korisnike
Nadzor, kontrola i revizija efektivnosti sistema zaštite i evaluacija usklađenosti politike i prakse zaštite	Nadzor, kontrola i revizija faktora smanjenja rizika i indikacije efektivnosti sistema zaštite
	Korišćenje rezultata evaluacije za usmeravanje aktivnosti i uspostavljanje odgovornosti menadžmenta
	Održavanje spremnosti za uvođenje novih tehnika i alata za nadzor, kontrolu i reviziju sistema zaštite

1.2.2. Uloge i odgovornosti

U organizaciji procesa za upravljanje zaštitom, uloge i odgovornosti se definišu i dodeljuju svim učesnicima u zaštiti, od glavnog menadžera do zaposlenih [1]. Za ISMS se imenuje menadžer za upravljanje informacijama – **CIO** (*Corporate Information Officer*),

ali je u velikim organizacijama trend da se ovom poslu posveti puno radno vreme, kao što je menadžer za sistem zaštite informacija – **CISSO** (*Corporate Information System Security Officer*), koji je odgovoran za zaštitu informacija u celoj organizaciji. Tendencija je podizanja odgovornosti za upravljanje zaštitom na viši nivo, u vidu profesionalnog menadžera za bezbednost informacija – **CIAO** *(Corporate Information Assurance Officer),* ovlašćenog i za sertifikaciju sistema zaštite [18].

Najznačajniji resurs za upravljanje zaštitom, na raspolaganju svakom menadžeru zaštite, svakako je tim dobro obučenih specijalista zaštite (**CIRT**), sa različitim i specifičnim znanjima, veštinama i iskustvima, relevantnim za lokalnu sredinu. Najbolja praksa zaštite zahteva da svaki član tima neprekidno usavršava znanja i veštine, u skladu sa zahtevima organizacije i ličnim potrebama. U ovoj oblasti apsolutno je potrebno *proaktivno* delovanje, pošto je veoma teško definisati i izvršiti strateški plan zaštite, ako su česte promene zaposlenih u IKTS i CIRT. Samo jedinstven i dobro obučen tim garantuje postizanje strateških bezbednosnih ciljeva. Pri tome je važno praviti razliku između znanja i veština, raspoloživih na tržištu i specifičnih veština i iskustava potrebnih za datu organizaciju i okruženje. Prvi tip se odnosi na opštu praksu zaštite, poznavanje principa, metodologija, koncepata, modela, tehnologija i alata zaštite, a stiču se, uglavnom, u obrazovnom sistemu i na brojnim kursevima zaštite (**CISSP –** *Certified Information System Security Professionals,* **SANS** i dr.). Drugi tip znanja i veština poseduje mali broj ljudi i najčešće su nedokumentovana i nedostupna širem krugu profesionalaca u zaštiti. Obe kategorije znanja i veština u zaštiti podjednako su značajne, s tim da je specifično obučene i iskusne specijaliste zaštite teže pronaći, zaposliti i zadržati.

1.2.3. Generički proces upravljanja zaštitom informacija

Generički proces upravljanja zaštitom informacija (IKTS) je ciklički ponovljiv i sadrži brojne potprocese, od kojih su glavni: *upravljanje rizikom, upravljanje promenama i upravljanje konfiguracijom*. Proces upravljanje rizikom i njegovi potprocesi analize i procene rizika su suštinski procesi upravljanja reaktivnim sistemom zaštite. Upravljanje promenama je proces koji pomaže da se identifikuju bezbednosni zahtevi kada se dogode promene u IKTS i okruženju. Upravljanje konfiguracijom je proces koji održava trag promena u IKTS, a može se izvršiti formalno i neformalno. Primarni cilj je da obezbedi da promene u sistemu ne smanjuju efektivnost sistema zaštite i ukupne bezbednosti organizacije.

Generički proces upravljanja zaštitom informacija dobro je definisan *klasom upravljačkih kontrola zaštite* u standardima ISO/IEC 27001: Anex A i NIST SP 800–53 A, B, C rev., koja obuhvata sledeće familije kontrola zaštite: *upravljanje programom, bezbednosnu procenu i autorizaciju, planiranje sistema zaštite, analizu i procenu rizika, akviziciju sistema i servisa zaštite*. U IKTS gde ne postoje implementiran ISMS, moraju se uključiti najmanje sledeće upravljačke kontrole: *razvoj politike zaštite, obuka i razvoj*

svesti o potrebi zaštite, upravljanje korisničkim nalozima, izveštavanje o incidentima i definisanje odgovornosti i saradnje u oblasti zaštite [21].

Generalno, moguća su dva *struktuirana prist*upa upravljanju zaštitom informacija. *Prvi* obuhvata upravljanje određenim brojem infrastrukturnih servisa, koji obezbeđuju normalan rad sistema zaštite. Osnovni nedostatak je što kompleksnost savremenih IKTS dovodi do postepene degradacije efektivnosti servisa IKTS i sistema zaštite, ako procesi upravljanja zaštitom i IKTS nisu dobro organizovani i sinhronizovani. *Drugi pristup,* pogodan za manje organizacije, je integrisano upravljanje sa IKTS i sistemom zaštite, gde mehanizmi zaštite obezbeđuju visoku raspoloživost IKTS servisa, a integrisano upravljanje – usklađeno funkcionisanje pod kontrolom administratora sistema.

Generički proces **ISMS** u osnovi sadrži četiri koraka: *identifikovanje pretnji, procena rizika, uspostavljanje politike zaštite i implementacija kontrola zaštite* za ublažavanje rizika (Sl. 1.1a). Druga opcija, za razvoj sistema za upravljanje zaštitom na strateškom nivou, na bazi konzistentne primene politike zaštite, je korišćenje standardnog *sistema identifikatora zaštite informacija* – **ISBS** (*Information Security Benchmark System*), koji predstavlja preporučeni nivo izvršavanja politike zaštite u normalnom okruženju i garantuje implementaciju dobrog sistema zaštite. Takođe, ISBS usaglašenost garantuje da je organizacija imala dobru procenu rizika i da je implementirala adekvatne kontrole zaštite za ublažavanje rizika (Sl. 1.1b) [5].



Sl. 1.1. Generički proces ISMS – (a) i usaglašenosti sa BS – (b)

Struktuirani integrisani proces upravljanja zaštitom informacija, prema standardu ITU X.700, obuhvata pet funkcionalnih oblasti upravljanja IKTS [10]: (1) *upravljanje konfiguracijom,* (2) *upravljanje otkazima*, (3) *upravljanje funkcionisanjem*, (4) *upravljanje zaštitom* i (5) *upravljanje kontrolnim informacijama*.

U *OOM upravljanja* uvodi se pojmovi *objekta upravljanja*, *atributi objekta, dopuštene operacije, izveštavanje i veza sa drugim objektima upravljanja*. U skladu sa preporukama (ITU X701), podsistem upravljanja sa distribuiranim IKTS uspostavlja se prema *klijent-server modelu*. *Klijent* je agent upravljanja koji vrši aktivnosti i dostavlja izveštaje o izmenama u procesu upravljanja. *Server* je menadžer koji daje agentu naredbe za upravljanje i prima izveštaje. Generički proces OOM upravljanja IKTS i sistemom zaštite informacija, obuhvata sledeće oblasti upravljanja:

- *informacionu*: atributi, operacije i izveštaji o objektima upravljanja,
- *funkcionalnu*: upravljanje aktivnostima i neophodnim informacijama,
- *komunikacionu*: komunikacioni aspekti upravljanja i obim informacija i
- *organizacionu*: dekompozicija na oblasti upravljanja.

Ključnu ulogu u ovom modelu upravljanja igra *OOM upravljačkih informacija* (ITU X720) koji podržava *inkapsulciju* i *nasleđivanje*. Dodatno se uvodi pojam *paketa* kao skup atributa, operacija, izveštaja i odgovarajućeg ponašanja [10].

1.2.4. Sistem upravljanja zaštitom informacija

Sistem upravljanja zaštitom informacija – **ISMS** je fokusiran na 12 komponenti zaštite i primenljiv na brojne industrijske oblasti, uključujući finansije, zdravstvo, vladu i komercijalni sektor. Iako se ISMS široko primenjuje, često nije jedini standard, koji organizacije primenjuju. Na primer, kompanije ga mogu koristiti za platne kreditne kartice, ali kako procesiraju, skladište ili prenose podatke sa platne kartice, mogu koristiti i implementirati industrijski fokusiran **PCI–DSS** (*Payment Card Industry Data Security Standard*) ili **BITS** (*Shared Assessment Program)*, SAD fondacija za finansijske servise, kao deo upravljačkog okvira [4, 5].

Standard ISMS, implementiran u skladu sa GAISP principima, predstavlja skup politika, procedura i uputstava za upravljanje zaštitom informacija ili upravljački okvir na bazi politike zaštite. ISMS je kompleksan sistem koji predstavlja sinergiju *tehničkih* i *proceduralnih kontrola* zaštite. Implementacija ISMS podrazumeva i uspostavljanje različitih tela u organizaciji (npr. *CIRT, forum, tim* ili *odeljenje za zaštitu informacija*) odgovornih za upravljanje procesima zaštite.

Ključni koncept uvođenja ISMS je dizajn, implementacija i dosledno sprovođenje procesa za efikasno upravljanje zaštitom CIA informacija i ublažavanja rizika na prihvatljiv novo. ISMS uređuje ponašanje zaposlenih, procese i tehnologije u zaštiti. Svaka organizacija uspostavlja svoj jedinstveni ISMS, koji će na optimalan način funkcionisati

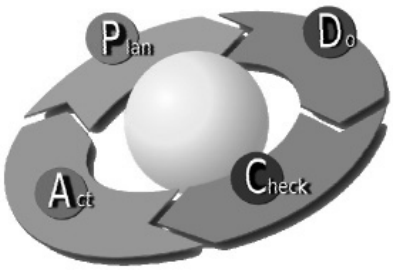
i obezbediti realizaciju poslovnih ciljeva. ISMS postavlja različita pravila, u zavisnosti od vrednosti informacione imovine i kulture rada. Fleksibilan je i može se efikasno implementirati u organizacijama različitih veličina, sa različitim potrebama i informacijama. Iako je fokusiran na upravljanje zaštitom informacija, nezavisno od tipa i formata informacija, ISMS podleže svim zakonima države i na taj način posredno obuhvata sve oblasti zaštite informacione imovine.

1.2.4.1. Uspostavljanje ISMS

Prvi korak u uspostavljanju ISMS–a je određivanje obima i konteksta u organizaciji, pri čemu nije uvek neophodno integrisati ISMS u sve segmente poslovanja. Moguće je u jednom projektu uspostaviti ISMS samo za određeni deo organizacije, što znatno smanjuje resurse. Za kontekst ISMS–a minimimalno se moraju uzeti karakteristike i način organizacije poslovanja, kako bi se obuhvatili svi neophodni procesi i delovi organizacije. Saopštenje o obimu ISMS može izgledati kao: *ISMS pokriva sve poslovne procese i resurse povezane sa IKTS i servisima koji se koriste za pružanje usluga u (naziv i lokacija organizacije)*. Pod tim se podrazumeva i funkcionisanje komunikacije do radne stanice *klijenta*. Ovo je u saglasnosti sa saopštenjem iz *Izjave o primenljivosti* (SOA), obaveznog dokumenta za sertifikaciju ISMS–a, gde se jasno vidi obim uspostavljanja ISMS–a. SOA obično nije javni dokument, da se organizacija ne bi izložila riziku, zbog informacija koje sadrži [23].

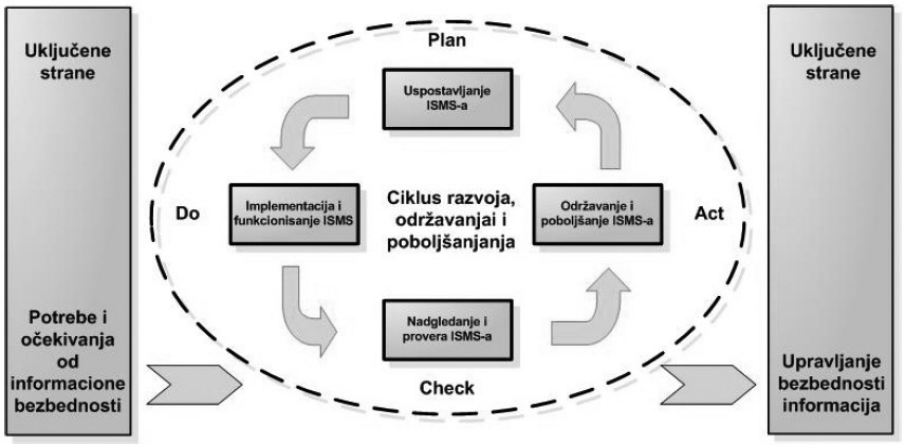
Iako gotovo svaka organizacija uspostavlja jedinstven ISMS u specifičnom kontekstu, upravljanje zaštitom informacija ima nekoliko zajedničkih elemenata, zasnivanih na konceptu ciklusa neprekidnog poboljšavanja procesa zaštite, odnosno, modelu *planiraj, implementiraj, proveri, deluj* – **PDCA**[29] (*Plan, Do, Check, Act*) ciklusa, kojeg čine faze **planiranja** – određuje kontekst, obim i granice ISMS i analizira i procenjuje rizik u odnosu na vrednosti informacione imovine; **implementacije –** realizuje odluke za uspostavljanje i implementaciju dizajna ISMS; **provere** – pratiti aktivnosti u praksu ISMS, otkriva propuste i slabosti i definiše neophodne promene i faza **delovanja,** koja realizuje promene na osnovu utvrđenih propusta (Sl. 1.2).

Unutar faza PDCA *Deming* je predvideo cikluse (tzv. *točak unutar točka*), koji povezuju *strategijski* menadžment i menadžment na nižem nivou u velikim kompanijama. Nakon završetka PDCA ciklusa, otpočinje novi i na taj način se upravljanje sistemom konstantno prilagođava potrebama organizacije (Sl. 1.3).



Sl. 1.2. PDCA (Plan, Do, Check Act) model [23]

29 Dr Edwards Deming, *Out of the crisis,* gde preporučuje PDCA model Walter A. Shewart-u, osnivaču statističke kontrole kvaliteta.



Sl. 1.3. Primena PDCA modela na ISMS prema ISO/IEC 27001

Uspostavljanje ISMS nužno dovodi do promena i utiče na sve aspekte organizacije. *Menadžment* organizacije obezbeđuje sve neophodne resurse za implementaciju, funkcionisanje i održavanje ISMS, a da pri tom ne utiče na osnovno poslovanje. *Zaposleni/korisnici* najčešće se moraju dodatno obučavati za primenu zahteva ISMS, da bi prihvatili promene u odnosu na stari način rada. *Klijenti/korisnici* moraju prihvatiti drugačiji način isporuke računarskih servisa zbog promena nastalih implementacijom ISMS. *Kultura rada* se menja, što posebno utiče na najstarije zaposlene, koji imaju izgrađene radne navike, a suočeni sa novim pravilima ponašanja, mogu ispoljiti pad morala tokom implementacije i primene ISMS. *Obavezno vlasništvo* nad objektima informacione imovine, može izazvati stres kod odgovornih zaposlenih. *Normativi* mogu zahtevati dodatno angažovanje zaposlenih za pisanje politike zaštite, koja mora biti usklađena sa nekim od zakona u državi. *Kritični faktori* za efikasno uvođenje ISMS–a u organizaciju mogu biti:

- usklađenost politike, ciljeva i prakse zaštite sa zahtevima poslovanja,
- konzistentnost sa kulturom rada i korisnička prihvatljivost ISMS,
- integrisanje svih uloga u ISMS u redovno poslovanje organizacije,
- menadžerska podrška, tako da zaposleni ozbiljno shvate procese ISMS,
- razumevanje svih zaposlenih o značaju zaštite i uticaju na poslovanje,
- razvoj svesti svih zaposlenih o potrebi zaštite, riziku i kako ga ublažavati,
- potpuna komunikacija između tima za uvođenje ISMS i ostalih zaposlenih,
- neprekidna obuka i edukacija zaposlenih u oblasti zaštite i
- procesni pristup, upravljanje i poboljšavanje procesa PDCA modela i ISMS.

1.2.4.2. Administracija sistema zaštite

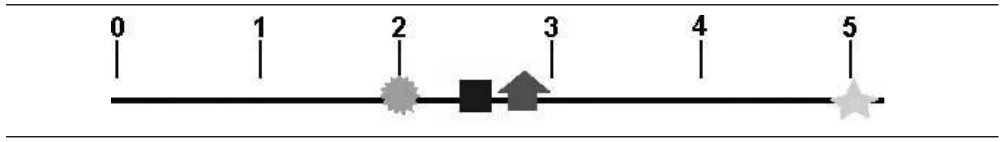
Administracija sistema zaštite u distribuiranom IKTS, uključuje prikupljanje, analizu i raspodelu informacija, neophodnih za rad servisa i mehanizama zaštite. Primeri su distribucija kriptografskih ključeva, analiza parametara zaštite, konfigurisanje log datoteka itd. Konceptualna osnova administracije zaštite je baza informacija za upravljanje zaštitom, koja može da postoji kao jedinstveni ili distribuirani repozitorijum. Svaki od implementiranih sistema treba da raspolaže informacijama, neophodnim za implementaciju izabrane politike zaštite. U skladu sa preporukama ITU X.800 zadaci se dele na administraciju *sistema, servisa i mehanizama zaštite* [10].

Administracija sistema zaštite u IKTS uključuje implementaciju aktuelne politike zaštite, saradnju sa drugim administratorima (sistema, mreže itd.), reagovanje na incidente, internu i eksternu reviziju, uspostavljanje i održavanje bezbednosnog stanja IKTS. *Administracija servisa zaštite* obuhvata bezbednosnu klasifikaciju i kategorizaciju informacione imovine, definisanje kriterijuma za izbor mehanizama za realizaciju servisa zaštite i saradnju sa drugim administratorima za usaglašavanje servisa zaštite. *Administracija mehanizama zaštite* određuje se na bazi skupa implementiranih mehanizama zaštite, a tipično obuhvata aktivnosti, kao što su *upravljanje ključem* (generisanje i distribucija), *upravljanje kriptozaštitom* (uvođenje, sinhronizacija i administracija kriptografskih parametara i mehanizama itd.), *upravljanje identitetom i pristupom* (distribucija lozinki, ključeva, smart kartica, ACL itd.), *upravljanje dopunom saobraćaja* (razrada i podrška pravila, izdavanje karakteristika dopune saobraćaja – frekvencije, obima itd.), *upravljanje rutiranjem saobraćaja* (dodeljivanje poverljivih kanala veze) i *upravljanje registrima* (distribucija informacija i administriranje servisa).

1.2.4.3. Metrika za evaluaciju upravljanja sistemom zaštite

Za određivanje efektivnosti i efikasnosti ISMS procesa, uvodi se metrika performansi procesa upravljanja. Kriterijumi za izbor metrike ISMS procesa mogu biti brojni parametri kao što su: *broj većih incidenata; broj implementacija, koje kasne iz bezbednosnih razloga; broj kritičnih poslova zavisnih od IKTS sa planom za kontinuitet poslovanja; broj kritičnih objekata infrastrukture IKTS sa automatskim nadzorom; procenat poboljšanja svesti o etičkim i principima zaštite; potpuna usaglašenost ili dopuštena odstupanja od bezbednosnih zahteva; procenat razvoja i dokumentovanja plana i politike zaštite* itd.

Kako ISMS standard ne nudi nikakvu metriku za merenje performansi ISMS procesa, može se koristiti model progresivnog sazrevanja procesa zaštite – SSE CMM (ISO/IEC 21827), specifično primenjen na procese upravljanja zaštitom [22]. Skala nivoa sazrevanja prikazana je na Sl. 1.4, gde je:



Sl. 1.4. Skala sazrevanja procesa upravljanja

0. NIVO: *ne postoji* — proces upravljanja zaštitom nije implementiran.
1. NIVO: *inicijalni proces* — procesi upravljanja su *ad hoc* i neregularni.
2. NIVO: *ponovljiv* — procesi upravljanja slede regularni obrazac i ponovljivi su.
3. NIVO: *definisan* — procesi upravljanja su ponovljivi, definisani i dokumentovani.
4. NIVO: *upravljan* — procesi upravljanja su nadzirani i kvantitativno mereni.
5. NIVO: *optimizovan* —primenjuje se najbolja praksa upravljanja zaštitom.

Izlazni rezultati procesa upravljanja zaštitom informacija mogu se grupisati u četiri osnovne oblasti**:**

1. strategijsko usklađivanje bezbednosnih i poslovnih zahteva,
2. novu poslovnu vrednost obezbeđuje set najboljih praksi zaštite,
3. upravljanje rizikom obezbeđuje prihvaćen i usaglašen profil rizika,
4. merenje performansi procesa upravljanja zaštitom definisanom metrikom.

1.2.5. Otvoreni problemi upravljanja zaštitom informacija

Osnovni problemi upravljanja zaštitom spadaju u dve glavne kategorije: *dobijanje neophodne podrške menadžerske strukture* za izvršavanje strateškog plana implementacije ISMS i *dobijanje neophodne podrške* zaposlenih organizacije za implementaciju politike zaštite [1, 10, 23, 25, 55].

U teoriji i praksi zaštite evidentirani su otvoreni problemi u **proceni ranjivosti** i to: *razumevanje stvarnog uticaja ranjivosti i rizika za IKTS u realnom okruženju; otežan rad administratora u analizi obimnih izveštaja o ranjivosti sistema; značajno kašnjenje razvoja bezbednosnih popravki i korekcije ranjivosti i; potrebno je više istraživanja rešenja proaktivne zaštite*, kao što su:

a. standardizacija alata za procenu ranjivosti sistema (*Nmap, Nessus Security, Scanner, ISS Internet Security Scanner, Symantec – NetRecon* itd),
b. usklađenost standardizacionih tela za procenu ranjivosti (**CIDF** – *Common Intrusion Detection Framework*, **IETF** – *International Engineering Task Force,* **IDWG** – *Intrusion Detection Working Group*, **CVE** – *Common Vulnerabilities and Exposures*...),
c. izvođenje važnih projekata za procenu ranjivosti: **CVE** lista standardnih imena za javno poznate ranjivosti i druge izloženosti sistema [32] i
d. usvajanje standardnog formata izveštaja o analizi ranjivosti – ARF (*Vulnerability Assesment Report Format*) [61].

U oblasti monitoringa zaštite i IDPS nedostaju: standardizacija interoperabilnosti i usaglašavanje tela za standardizaciju; identifikovanje ograničenja i tekućih problema IDPS; otvorena pitanja filtriranja ličnih i podataka o organizaciji iz sirovih podataka u procesima zaštite privatnosti, analize ranjivosti i monitoringa IDPS; kompromis između zahteva za privatnost i kapaciteta IDPS; deljenje podataka izvan domena zaštite, sa održavanjem privatnosti; uvođenje analize ranjivosti/privatnost (**SPVA**) slično analizi ranjivosti/pretnje i dr.

1.2.6. Preporuke za upravljanje zaštitom informacija

Standard ISMS sugeriše da svaka organizacija treba da definiše, implementira, dokumentuje i održava najmanje sledeće [23]:

- **obim i granice ISMS** (4.2.1a) i **bezbednosne ciljeve** (4.3.1a);
- **ISMS Politiku,** kao okvir za set pravila komponenti zaštite (4.2.1b);
- opis **pristupa** (4.2.1c) ili **metodologije** (4.3.1d);
- **izveštaj o proceni rizika,** koji identifikuje informacionu imovinu u opsegu ISMS, pretnje, iskoristivosti i uticaje koji mogu dovesti do gubitka CIA (4.2.1c,d,e,f,g i 4.3.1e);
- **plan ublažavanja rizika,** koji identifikuje evaluirane opcije za tretman faktora rizika (4.2.1f i 4.2.2b);
- **prihvatanje preostalog rizika i akreditaciju ISMS,** čime menadžment prihvata preostali rizik i odobrava primenu ISMS (4.2.1h i 4.2.1i);
- **izjavu o primenljivosti** (*SOA*)**,** koja definiše ciljeve izabranih kontrola i kontrole sa razlozima njihovog izbora, identifikuje ciljeve tekućih i implementiranih kontrola i dokumentuje razloge za isključivanje bilo kojeg cilja kontrola zaštite (4.2.1g, Aneks A, koji sumira kontrole iz ISO/IEC 27002);
- **dokumentovanje procedura** za efektivno planiranje, operativno upravljanje i kontrolu procesa zaštite i opis metrika efektivnosti kontrola zaštite (4.3.1g);
- **evidencije operativne primene ISMS**, kao što su odluke menadžera, rezultati sistema nadzora i procedura revizije (*audit*–a), procene rizika, izveštaja interne kontrole i revizije – ISMS, plana itd. (4.2.3, 4.3.1 i 4.3.3).

Standard ISO/IEC 27001 sugeriše izradu najmanje sledećeg skupa politika/pravila zaštite (lista nije zaključena):

1. sveobuhvatna ISMS Politika (*ISMS Policy*);
2. politika kontrole pristupa (*Access Control Policy*) ;
3. politika čistog stola i ekrana računara (*Clear Desk and Clear Screen Policy*) ;
4. politika arhiviranja i zadržavanja podataka (*Data Archive And Retention Policy*);
5. politika klasifikacije informacija (*Information Classification Policy*);
6. politika odlaganja informacija / medija / opreme (*Disposal of Information / Media / Equipment Policy*);
7. politika zaštite elektronske trgovine (*eCommerce Security Policy*);
8. politika prihvatljive upotrebe e–pošte (*E–mail Security/Acceptable Use Policy*);
9. politika procene rizika bezbednosti informacija (*Information Security Risk Assessment Policy*);

10. politika zaštite laptop računara (*Laptop Security Policy*);
11. politika mobilnog računarstva i telerada (*Mobile Computing and Teleworking Policy*);
12. politika zaštite iznajmljenih resursa (*Outsourcing Security Policy);*
13. politika upravljanja lozinkom (*Password Policy*);
14. politika testiranja na proboj (*Penetration Testing Policy*);
15. politika personalne zaštite (*Personnel Security Policy*);
16. politika fizičke zaštite (*Physical Security Policy*);
17. politika zaštite privatnosti (*Privacy Policy*);
18. politika zaštite autorskih prava na softver (*Software Copyright Policy*);
19. politika zaštite od spama (*Spam Policy*);
20. politika oporavka i bekapovanja sistema/podataka (*System/data Backup and Recovery Policy*);
21. politika nadzora korišćenja sistema (*System Usage Monitoring Policy*);
22. politika udaljenog pristupa treće strane (*Third Party Access Policy*);
23. politika zaštite od virusa/malicioznih programa (*Virus/malware Policy*).

Preporučene procedure zaštite informacija daju smernice za procese uključene u implementaciju kontrola zaštite informacija:

1. procedura bekapovanja;
2. procedure revizije i procene usaglašenosti;
3. procedura izveštavanja o incidentu;
4. procedura revizije logičke kontrole pristupa;
5. procedura upravljanja bezbednosnim zakrpama;
6. procedura administracije zaštite;
7. procedura ojačavanja sistema (*System Hardening Procedure*);
8. procedura testiranja sistema zaštite;
9. procedura za korisničko održavanje.

Procedure za upravljanje ISMS, koje obezbeđuju smernice za uključene procese:

1. procedure za korektivne/preventivne akcije;
2. procedura za kontrolu i reviziju evidencija i dokumenata;
3. procedura interne kontrole ISMS;
4. materijali za razvoj svesti o potrebi zaštite informacija;
5. uputstvo za reviziju ISMS;
6. radna tabela za analizu rizika bezbednosti informacija*;*
7. radna tabela za FMEA analizu rizika (koristi modele grešaka i analizu efekata, sa fokusom na potencijalne posledice) itd.

Preporučeni profili profesija u oblasti zaštite informacija (uloge, odgovornosti, kompetencije itd.) za poslove u ISMS:

1. uloge za planiranje kontinuiteta poslovanja i oporavak sistema;
2. vlasnik informacione imovine (*Information Asset Owner*);
3. analitičar zaštite informacija (*Information Security Analyst*);
4. projektant sistema zaštite (*Information Security Architect*);
5. menadžer zaštite informacija (*Information Security Manager*);
6. referent (specijalista) zaštite informacija (*Information Security Officer*);
7. verifikator (tester) zaštite informacija (*Information Security Tester*);
8. revizor IKTS (*ICT Auditor*);
9. administrator zaštite (*Security Administrator*).

Preporučene formalne evidencije u primeni ISMS):

1. planovi za kontinuitet poslovanja i izveštaji o testiranju/vežbama;
2. izveštaji i liste provera za procenu uticaja na poslovanje;
3. planovi za oporavak IKTS od vanrednih događaja i izveštaji o testiranju/vežbama;
4. obrasci za izveštavanje i izveštaji o kompjuterskom incidentu;
5. revizija lista za proveru arhitekture i dizajna tehničkog rešenja zaštite;
6. liste za provere/upitnici za pretnje i ranjivosti.

ISMS radna dokumenta:

1. registar bekapovanja/arhiviranja (detalji o mediju, podacima, tipovima i obimu);
2. registar plana za kontinuitet poslovanja (detalji o svim BCP – status, vlasništvo, obim, datum poslednjeg testiranja itd.);
3. baza podataka/registar inventara informacione imovine;
4. registar faktora rizika bezbednosti informacija (naziv, vlasnik i priroda rizika, odluka menadžmenta za redukciju/transfer/izbegavanje/rizika itd.);
5. registar kompjuterskih incidenata (može se derivirati iz log datoteka);
6. lista privilegovanih/administratorskih pristupa i ovlašćenja;
7. registar licenciranih programa (snabdevač, tip i uslovi licence/restrikcije, vlasnik/menadžer odnosa sa snabdevačem);
8. lista standardnih programa desktop računara (katalog dozvoljenih sistemskih i aplikativnih programa za desktop računare);
9. registar sistemskih zakrpa i statusa AVP (verovatno automatizovan);
10. registar kontakata i pristupa TTP (ugovorne, kontaktne i druge informacije o TTP).

1.3. REZIME

U procesu upravljanja, GAISP čini osnovni skup konzistentnih principa za *upravljanje sistemom zaštite* informacija ili za *integralno upravljanje* IKTS sa implementiranim (pod)sistemom zaštite. *Upravljanje sistemom zaštite* odnosi se na određeni broj infrastrukturnih servisa koji obezbeđuju normalni rad komponenti zaštite i IKTS u celini. Najznačajniji resurs menadžera za upravljanje zaštitom je tim specijalista zaštite (CIRT).

Integralno upravljanje sa IKTS i sistemom zaštite (ITU X.700) integriše skupove informacionih servisa i servisa zaštite, gde mehanizmi zaštite obezbeđuju visoku raspoloživost informacionih servisa, a upravljanje pouzdan rad i usklađeno funkcionisanje oba skupa pod kontrolom administratora sistema. Proces obuhvata *monitoring*, reviziju i *koordinaciju* komponenti podsistema upravljanja. U skladu sa ITU X.800 zadaci administracije zaštite dele se na tri oblasti – administraciju *IKTS, servisa i mehanizama zaštite*.

Dobru metodologiju za uspostavljanje procesa za upravljanje zaštitom informacija obezbeđuje standard IEC/ISO 27001 (ISMS). Glavni cilj upravljanja zaštitom informacija je uspostavljanje održivog programa, selekcija i izbor potrebnih resursa i revizija sistema zaštite za održavanje rizika na prihvatljivom nivou. Osnovna komponenta programa zaštite je *politika zaštite* zasnovana na proceni rizika, koja odražava spremnost organizacije da štiti svoje informacije. Za merenje performansi procesa upravljanja uspešno se koristiti metrika modela sazrevanja procesa zaštite (SSE – CMM): 0 – *ne postoji,* 1 – *inicijalni proces,* 2 – *ponovljiv*, 3 – *definisan,* 4 – *kvantitativno upravljan,* 5 – *optimizovan)*.

Osnovni problemi upravljanja zaštitom su obezbeđivanje podrške menadžerske strukture za izvršavanje strateškog plana i korisničke prihvatljivosti za realizaciju politike zaštite. Preporuke za efektivno upravljanje sistemom zaštite informacija (ISMS) obezbeđuje standard ISO/IEC 27001. Otvoreni su brojni problemi u oblasti usklađivanja i standardizacije tehnika upravljanja i izveštavanja rezultata procesa zaštite (evaluacije, procene ranjivosti, validacije izlaza IDPS sistema i dr.).

1.4. KLJUČNI TERMINI

Administracija zaštite: uključuje realizaciju politike zaštite, saradnju sa drugim administratorima, reagovanje na incidente, nadzor i kontrolu sistema zaštite.

Administracija mehanizama zaštite: određuje se na bazi skupa implementiranih mehanizama zaštite i obuhvata brojne aktivnosti, koje opisuju procedure.

Administracija servisa zaštite: obuhvata klasifikaciju i određivanje objekata zaštite, izradu pravila za izbor mehanizama zaštite i saradnju sa drugim administratorima.

Administracija zaštite u distribuiranom sistemu: dodatno uključuje prikupljanje i raspodelu informacija neophodnih za rad servisa i mehanizama zaštite.

Izjava o primenljivosti – SOA (*Statement Of Applicability*): dokument kojim menadžment potvrđuje i prihvata primenljivost ili neprimenljivost kontrola za tretman rizika.

Upravljanje sistemom zaštite: određeni broj infrastrukturnih servisa koji obezbeđuju normalni rad komponenti, uređaja i sistema zaštite informacija.

Zapis (*Record*): evidencija objektivnog dokaza koji pokazuje da je aktivnost preduzeta.

1.5. PITANJA ZA PONAVLJANJE

1. Za upravljanje zaštitom mogu se primeniti sledeći principi upravljanja rizikom:
   a. procena rizika i određivanje bezbednosnih potreba
   b. uspostavljanje organizacije za centralno upravljanje
   c. GAISP principi zaštite
   d. implementacija politike i rentabilnih kontrola zaštite
   e. razvoj svesti o potrebi zaštite i obuka korisnika u zaštiti
   f. nadzor i revizija efektivnosti sistema zaštite i evaluacija usklađenosti
   g. sertifikacija i akreditacija sistema zaštite
2. Ako u IKTS nije implementiran sistem zaštite, treba uključiti najmanje sledeće upravljačke kontrole:
   a. razvoj politike zaštite
   b. fizička zaštita
   c. obuka i razvoj svesti o potrebi zaštite
   d. nametanje obaveza i elementarna praktična obuka u oblasti zaštite
   e. personalna zaštita
   f. obavezna razmena informacija o incidentima
   g. definisanje i saradnja nosioca odgovornosti u oblasti zaštite
3. Prvi pristup upravljanja zaštitom informacija uključuje:
   a. tretira upravljanje zaštitom kao integralni proces IKTS i sistema zaštite
   b. određeni broj infrastrukturnih servisa koji obezbeđuju normalni rad IKTS i sistema zaštite
   c. mehanizmi zaštite obezbeđuju visoku raspoloživost informacionih servisa
   d. kompleksnost IKTS i sistema zaštite dovodi do postepene degradacije servisa IKTS i sistema zaštite, ako procesi nisu sinhronizovani
   e. integrisano upravljanje obezbeđuje normalno i usklađeno funkcionisanje pod kontrolom sistem administratora
   f. zahteva dobru organizaciju i sinhronizaciju upravljanja zaštitom i IKTS
4. Drugi pristup upravljanja zaštitom:
   a. tretira upravljanje sistemom zaštite kao integralni faktor IKTS i sistema zaštite
   b. obuhvata određeni broj infrastrukturnih servisa koji obezbeđuju normalni rad IKTS i sistema zaštite
   c. mehanizmi zaštite obezbeđuju visoku raspoloživost informacionih servisa
   d. kompleksnost IKTS i sistema zaštite dovodi do postepene degradacije servisa IKTS i sistema zaštite, ako procesi nisu sinhronizovani
   e. integrisano upravljanje obezbeđuje normalno i usklađeno funkcionisanje pod kontrolom sistem administratora
   f. zahteva dobru organizaciju i sinhronizaciju upravljanja zaštitom i IS

5. Klasa upravljačkih kontrola najbolje prakse zaštite sadrži sledeće familije kontrola:
   a. upravljanje konfiguracijom, upravljanje otkazima, upravljanje funkcionisanjem, upravljanje vanrednim događajem i incidentom
   b. upravljanje programom, bezbednosnu procenu i autorizaciju, planiranje sistema zaštite, analizu i procenu rizika, akviziciju sistema i servisa zaštite
   c. upravljanje zaštitom, upravljanje kontrolnim informacijama, planiranje sistema zaštite, analizu i procenu rizika, akviziciju sistema i servisa zaštite
6. U skladu sa standardom ISO/IEC 27001 za upravljanje sistemom zaštite informacija ključni koraci su:
   a. identifikovanje pretnji i procena rizika
   b. planiranje i delovanje
   c. provera i korekcije ranjivosti
   d. implementacija kontrola zaštite i uspostavljanje politike zaštite
7. Sistem identifikatora (benchmark) za razvoj upravljanja zaštitom informacija sadrži tri faze:
   a. Benčmark sistem, uspostavljanje politike zaštite, implementacija kontrola zaštite
   b. identifikovanje pretnji, procena rizika, uspostavljanje politike zaštite, implementacija kontrola zaštite
   c. Benčmark sistem, procena rizika, implementacija kontrola zaštite
8. Generički proces OOM upravljanja IKTS i zaštitom informacija obuhvata sledeće oblasti upravljanja:
   a. informacionu, programsku, komunikacionu i organizacionu
   b. informacionu, funkcionalnu, komunikacionu i organizacionu
   c. programsku, funkcionalnu, komunikacionu i organizacionu
   d. informacionu, strukturnu, komunikacionu i organizacionu
9. U skladu sa preporukama ITU X.700 strukturirani integrisani proces upravljanja obuhvata upravljanje:
   a. programom zaštite, konfiguracijom, otkazima, funkcionisanjem, topologijom mreže
   b. vanrednim događajem, kompjuterskim incidentom, konfiguracijom, otkazima, funkcionisanjem
   c. konfiguracijom, otkazima, funkcionisanjem, zaštitom i kontrolnim informacijama
   d. politikom zaštite, administracijom zaštite, otkazima, funkcionisanjem, fizičkom zaštitom i kontrolnim informacijama
10. U OOM upravljanja uvode se sledeći pojmovi:
   a. objekti upravljanja ključem (generisanje i distribucija), atributi objekta, dopuštene operacije, izveštavanje i veza sa drugim objektima upravljanja
   b. objekti upravljanja, atributi objekta, dopuštene operacije, izveštavanje i veza sa drugim objektima upravljanja
   c. objekti upravljanja rutiranjem saobraćaja, atributi objekta, dopuštene operacije, izveštavanje i veza sa drugim objektima upravljanja
11. Zajednički elementi sistema upravljanja zaštitom informacija (ISMS) su:
   a. pripremi, izaberi tim, uskladi sa politikom i implementiraj
   b. izbor tima za upravljanje zaštitom
   c. planiraj, implementiraj, proveri i deluj
   d. kontrola i revizija sistema zaštite
   e. planiraj, proceni rizik, izaberi kontrole, implementiraj i proveri
12. Osnovne kategorije preporuka i problema upravljanja zaštitom su:
   a. obezbeđivanje neophodne podrške menadžerske strukture
   b. obezbeđivanje tehničkih kontrola zaštite

c. obezbeđivanje potrebnog nivoa svesti o potrebi zaštite
d. obezbeđivanje potrebne podrške zaposlenih
e. obezbeđivanje tima za zaštitu

13. U skladu sa preporukama ITU X.800 zadaci administratora *zaštite IKTS u celini* su:
    a. saradnju sa drugim administratorima za usaglašavanje servisa zaštite
    b. izrada aktuelne politike zaštite
    c. upravljanje kriptozaštitom
    d. planiranje vanrednih događaja
    e. reagovanje na incidente
14. U OOM i procesnom pristupu, metrika za evaluaciju ISMS zasniva se na:
    a. metrici ISMS standarda
    b. metrici standarda ISO/IEC 13335–3
    c. metrici standarda ISO/IEC 21827
    d. metrici standarda ISO/IEC 15405
15. *Izlazni rezultati* procesa upravljanja zaštitom informacija mogu se grupisati u sledeće osnovne oblasti:
    a. zakonsko usklađivanje, novi kvalitet sistema zaštite, upravljanje rizikom, merenje performansi
    b. usklađivanje sa praksom zaštite, nova vrednost procesa zaštite, merenje performansi, upravljanje rizikom
    c. strategijsko usklađivanje, nova poslovna vrednost, upravljanje rizikom, merenje performansi
16. Povežite nivoe procesa upravljanja sa odgovarajućim karakteristikama:

Nivo zrelosti	Glavne karakteristike
0. nivo	*a. ponovljiv* — procesi upravljanja slede regularni obrazac i ponovljivi su
1. nivo	*b. definisan* — procesi upravljanja su dokumentovani, upoznata organizacija
2. nivo	*c. ne postoji* — proces upravljanja zaštitom nije uopšte primenjen
3. nivo	*d. inicijalni proces* — procesi upravljanja su *ad hoc* i neregularni
4. nivo	*e. optimizovan* —primenjuje se najbolja praksa upravljanja zaštitom
5. nivo	*f. upravljan* — procesi upravljanja su nadzirani i mereni

2. UPRAVLJANJE BEZBEDNOSNIM RIZIKOM

Po završetku ovog poglavlja moći ćete:

- Primeniti opštu metodologiju upravljanja rizikom
- Primeniti formalnu metodologiju procene/proračuna rizika
- Koristiti opšti metod za procenu:
  A – vrednosti informacione imovine
  T – pretnji
  V – ranjivosti
  U – uticaja kombinovanih *T* na *V*
  Rrp – preostalog prihvatljivog rizika

2.1. UVOD

Upravljanje bezbednosnim rizikom u IKTS, u suštini, obuhvata sveukupan proces uspostavljanja i održavanja reaktivnog sistema zaštite. Procena rizika, ključna komponenta upravljanja rizikom, je proces kojim se rizik identifikuje, analizira, evaluira i procenjuje, da bi se obezbedio adekvatan i rentabilan sistem zaštite.

Rizik je funkcija verovatnoće da će dati agent pretnje iskoristiti određenu ranjivost IKTS i izazvati negativne posledice za sistem i organizaciju u celini, a može biti *inherentni*, *tekući* i *preostali.* Nivo *prihvatljivog* rizika je specifičan za svaku organizaciju, zavisi od misije, internih standarda, vrednosti imovine, kulture rada i odluke menadžmenta. Što je opis rizika detaljniji, to ga je lakše razumeti i proceniti. Misija sistema zaštite je održavanje zaštite na prihvatljivom nivou rizika.

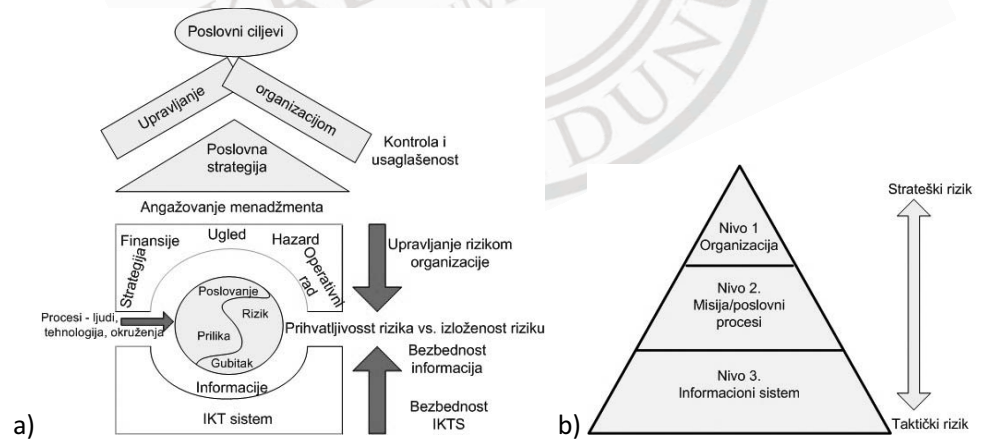
Procena rizika može se vršiti u svim fazama razvoja životnog ciklusa IKTS. Zavisno od namene, mere i metodi ublažavanja rizika mogu se svrstati u osam grupa: *izbegavanje rizika*, *transfer rizika*, *redukcija pretnji*, *redukcija ranjivosti sistema*, *redukcija uticaja pretnji*, *detekcija i sprečavanje pretnji, prihvatanje rizika i oporavak sistema.* Neke mere je lakše i jeftinije uvesti u ranoj fazi životnog ciklusa sistema. M*etod* za procenu rizika, razvijen na bazi generičke metodologije za analizu rizika – ISO/IEC TR 13335 – 3 i standarda ISO/IEC 27005, NIST SP 800 – 30, zahteva akviziciju informacija o *vrednosti informacione imovine* (**A)**, *pretnjama* (**T)**, *ranjivostima* (**V**), *uticaju* (**U**) ili proceni da će pretnje iskoristiti ranjivosti i potencijalno uticati na poslovne procese u vidu materijalne i/ili nematerijalne štete i o *proceni i proračunu faktora rizika* – kombinovanjem atributa **A, T, V i U**.

Za ublažavanje rizika biraju se i implementiraju *kontrole* zaštite, tako da obezbede *izbalansiranu i komplementarnu zaštitu*, tj. sistem zaštite u kojem su manje efikasne mere i metode zaštite dopunjene sa efikasnijim merama i metodama, a *tehničke* kontrole zaštite sa *proceduralnim.*

2.2. OPŠTA METODOLOGIJA ZA UPRAVLJANJE RIZIKOM

2.2.1. Glavni principi upravljanja rizikom

U modelu *strateškog rizika organizacije („kuće rizika")* (Sl. 2.1a)[30], iz perspektive izvršnog menadžmenta, uloga bezbednosti IKTS je minorna i od tima za zaštitu zahteva se da IKTS bude dobro zaštićen, a informacije dostupne, poverljive i neizmenjene. U isto vreme, informatičari znaju da je uloga IKTS odlučujuća, jer se većina, ako ne i sve informacije organizacije nalaze u sistemu. Drugim rečima, bez bezbednosti IKTS, informacioni blok *strateškog rizika* nije stabilan, kao ni čitav sistem. Gotovo svi poslovni IKTS u Internet okruženju, izloženi su sličnim bezbednosnim rizicima, koriste slične tehnologije za ublažavanje rizika i imaju slične ciljeve – *zaštitu CIA informacija*. Preporučuje se hijerarhijski pristup upravljanju rizikom, koji podrazumeva fleksibilnu i agilnu implementaciju, čvrsto povezanu sa arhitekturom i fokusiranu na ceo životni ciklus sistema. (Sl. 2.1b).

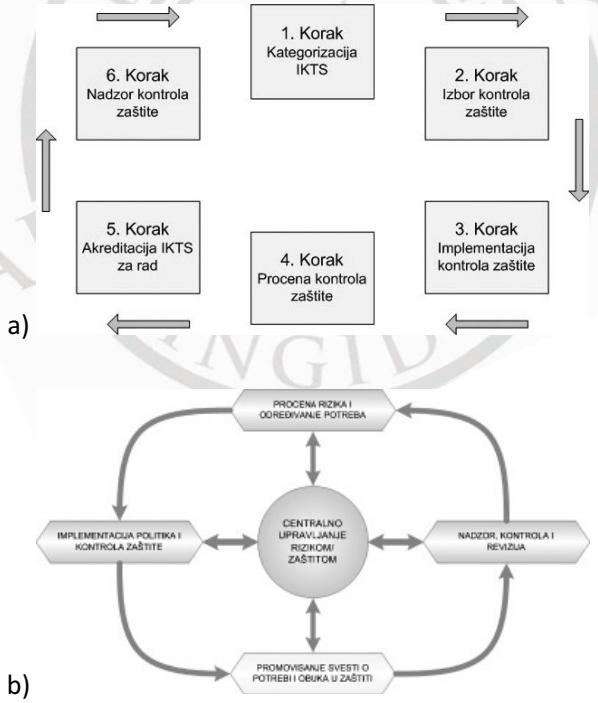


Sl. 2.1. Model – (a) i hijerarhijski pristup upravljanju strateškim rizikom – (b)

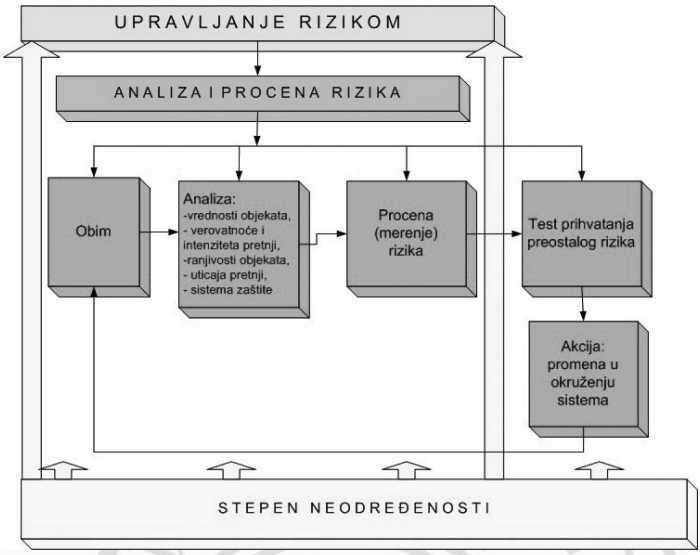
30 Bartol, N., & all, *Measuring Cyber Security and Information Assurance*, IATAC, 8. 05. 2009.

Funkcionalni model generičkog okvira za upravljanje rizikom prikazan je na Sl. 2.2a. Za efektivno upravljanje rizikom, treba implementirati šesnaest aktivnosti (videti Tabelu 1.1) glavnih principa upravljanja rizikom (UR). Važan faktor za efektivnu implementaciju principa UR je njihovo ciklično ponavljanje, koje obezbeđuje da politika zaštite uvek uključuje tekuće faktore rizika, približno u realnom vremenu. Ciklično upravljanje rizikom (Sl. 2.2b) obezbeđuje održavanje politike zaštite, nadzor, kontrolu, reviziju i upravljanje sistemom zaštite [67].

U OOM, IKTS i okruženje se razmatraju kao jedna celina, sa sledećim objektima: *ciljevi, okruženje, resursi, komponente i upravljanje* [10, 66]. Odnosi sistema i okruženja i stepen kontrole, koju neka organizacija može uspostaviti nad okruženjem sistema, zavise u najvećoj meri od obima i intenziteta skupljanja informacija, potrebnih za analizu i procenu faktora rizika. Opšti model za analizu i procenu bezbednosnog rizika sadrži tri konceptualne oblasti – *upravljanje rizikom*, *analizu* i *procenu rizika* i *stepen neodređenosti rizika* (pretnje, iskorišćenja ranjivosti i uticaja), koja interaktivno deluje na procenu faktora rizika (Sl. 2.3).



Sl. 2.2. Generički okvir – (a) i ciklus – (b) upravljanja rizikom

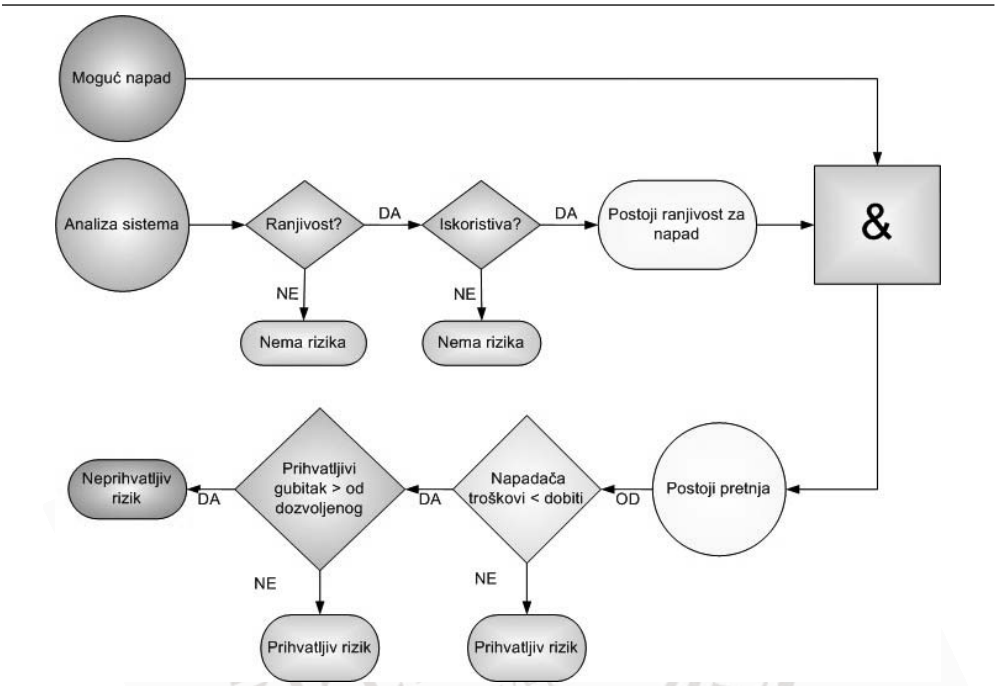


Sl. 2.3. Generički model za analizu i procenu rizika [67]

U prvom koraku definiše se obim procene rizika. Zatim se analiziraju komponente rizika – vrednost imovine (A), pretnje (T), ranjivosti (V), verovatnoća uticaja (U) i zaštita, kvantifikuju se njihovi atributi i specificiraju međusobni odnosi. Iz rezultata analize procenjuju se faktori rizika i testira njihova prihvatljivost. U analizi *uticaja* faktora rizika razvija se scenario *„šta ako“,* u slučaju da se dogodi svaki razmatrani faktor rizika. Procenjuju se verovatnoća pojave, učestanost i intenzitet uticaja svakog faktora rizika, kao i uticaja kombinacije faktora rizika. Procena faktora rizika je valjana za određeno vreme, iako se temeljito uradi, jer se scenario pretnji brzo menja pa se i procena rizika mora češće ažurirati. Ako su faktori rizika realni, proces ulazi u okvir upravljanja rizikom, gde se mogu specificirati promene zahteva za sistem ili okruženje sistema, uvođenjem različitih kontrola zaštite. Procedura se ponavlja sve dok svi analizirani faktori rizika ne budu tretirani ili na prihvatljivom nivou. Tok procesa upravljanja rizikom najbolje generiše kriterijume za izbor kontrola zaštite, rentabilnih za ublažavanje rizika, i to ako [55]:

- *napad postoji*: implementirati pouzdane tehničke kontrole za smanjenje verovatnoće neželjenog napada;
- *postoji iskoristiva ranjivost***:** primeniti slojevitu zaštitu i projektovati bezbednu arhitekturu IKTS da se spreči iskorišćenje ranjivosti;
- *troškovi napada su manji od dobiti*: primeniti takve kontrole zaštite da se povećaju troškovi napada ili značajno smanji potencijalna dobit napadača;
- *gubitak je suviše velik*: primeniti principe projektovanja i arhitekture sistema višeslojne zaštite sa proceduralnim i tehničkim kontrolama zaštite.

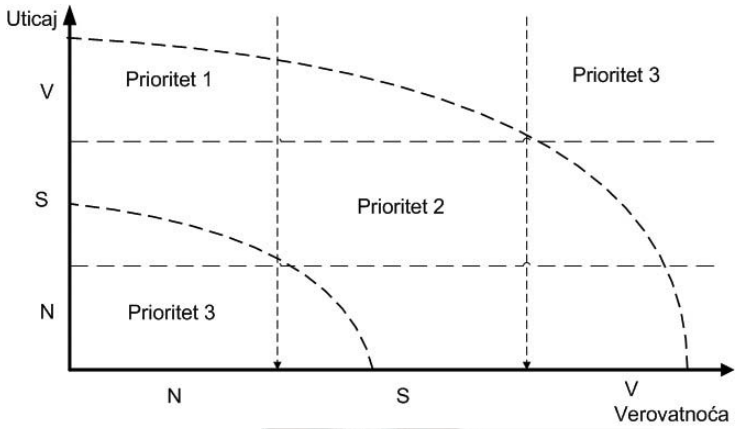
Primer toka procesa za uspešno održavanja rizika na prihvatljivom nivou za namerni, ali ne i maliciozni napad hakera sa Intraneta prikazan je na Sl. 2.4. [26].



Sl. 2.4. Tok procesa UR od namernog, nemalicioznog eksternog napada

2.2.2. Generički metod kvalitativne procene rizika

U procesu analize i procene bezbednosnog rizika, procenjuju se sledeći atributi: *vrednost informacione imovine* – **A**, *pretnje* – **T**, *ranjivosti* – ***V*** i *uticaj* – **U** (verovatnoća da će pretnje iskoristiti ranjivosti i naneti štetu)**.** Procene su uvek unutar obima i granica bezbednosnog rizika i smatra se da izvan njih nema rizika [49]. Atributima se pridružuju *kvalitativni* težinski faktori (numerički: 1 – 5; 1 – 10 itd. ili tekstualni: *nizak, srednji*, *visok; nizak, srednje nizak, srednji, srednje visok, visok* itd.) koji se, zatim, kombinuju, proizvodeći meru *relativnog rizika* – **Rr** za specifičnu ranjivost. Vrednost rizika se uvek smatra *relativnom***,** zato što se relacija zasniva na subjektivnom vrednovanju i rangiranju vrednosti atributa **A,T,V,U** bez formalnog proračuna faktora *neodređenosti* ovih atributa. Stohastička dimenzija rizika se u velikoj meri odnosi na to, koliko je za agenta pretnje atraktivno da iskoristi ranjivost sistema. Ova atraktivnost određuje prioritet akcije i direktno je proporcionalna odnosu uticaja i rizika ili verovatnoći neuspeha akcije, koju agent pretnje preduzima (Sl. 2.5).



Sl. 2.5. Dijagram odnosa „uticaj–verovatnoća neuspeha" napada

Koristan način za poređenje faktora rizika je, takođe, odnos koristi za napadača i rizika kojem se izlaže. Što je korist za napadača veća u odnosu na rizik, kojem se izlaže, iskorišćavanjem ranjivosti za napad na sistem, može se očekivati češća materijalizacija tog faktora rizika. Napadač nastoji da ostvari što veću korist uz što manji rizik i takav napad će biti prioritetan.

Za razumevanja procesa procene rizika korisno je razumeti prirodu i doprinos svakog pojedinačnog atributa ukupnom riziku, kroz primer intuitivne *kvalitativne procene* atributa **Rr** (Tabeli 2.1).

Tabela 2.1. Primer intuitivne procene atributa **A,V,T** i relativnog rizika (**Rr**)

Primer scenarija	Procena *A*	Procena *V*	Procena *T*	Procena *Rr*
Korpa sa mesom i vukovima u šumi	visoka	visoka	visoka	visoka
Prazna korpa sa vukovima u šumi	niska	visoka	visoka	niska
Meso u hermetički zatvorenom kontejneru sa vukovima u šumi	visoka	niska	visoka	niska
Korpa sa mesom na kuhinjskom stolu	visoka	visoka	niska	niska

2.2.3. Formalna metodologija za procenu rizika

Dva, svetski, najpoznatija entiteta za standardizaciju i najbolju praksu zaštite informacija (ISO/IEC 27005 i NIST SP 800-30), razvili su metodologiju za upravljanje rizikom kroz četiri različite aktivnosti: *procena rizika, ublažavanje rizika, prihvatanje rizika i ko-*

munikaciju rizika. ISO/IEC 27005 metodologija procene rizika sadrži tri glavne aktivnosti: identifikaciju, analizu i evaluaciju rizika. NIST standard predlaže sveobuhvatnu procenu rizika, koja uključuje devet primarnih koraka, koji se danas smatraju najboljom industrijskom praksom za procenu rizika: *(1) karakterizacija sistema, (2) identifikacija pretnji, (3) identifikacija ranjivosti, (4) analiza kontrola, (5) određivanje verovatnoće, (6) analiza uticaja, (7) određivanje rizika, (8) preporuke kontrola zaštite i (9) dokumentacija procene rizika*. Međutim, zbog faktora neodređenosti, sistemi zaštite bazirani na bilo kojoj metodologiji za procenu rizika, daju organizaciji samo privid da je zaštićena, jer se ne zasniva na stvarnom stanju rizika. Zato svaki tim za UR mora identifikovati razlike između privida i stvarnog stanja rizika IKTS i što efikasnije ih otklanjati [67, 24].

U poslednjim decenijama evolucije psihologije i neurologije, obezbeđeni su dokazi o ljudskoj percepciji rizika. Ljudi koriste različite *mentalne kalkulatore* koji ih, zavisno od toga na čemu se zasnivaju, čine dobrim ili lošim proceniteljima rizika. Ipak, čovek je, često, daleko od toga da sam izvrši realnu procenu rizika. Na primer, percepcija značaja rizika se povećava, čitajući o najgorim scenarijima u medijima, pri čemu se gubi iz vida verovatnoća tog događaja.

Pareto princip, poznat kao i pravilo **80:20**, odnosno, da 80% efekata dolazi od 20% uzroka, u potpunosti se može primeniti na procenu rizika: 80% posledica od realizacije rizika, dolazi od iskorišćenja 20% postojećih ranjivosti. Problem je u tome, kako identifikovati tih 20% postojećih ranjivosti. Grafikoni uticaj-verovatnoća i korist-rizik, mogu pomoći da se primeni *Pareto princip*. U odnosu na hroničan nedostatak sredstava za ublažavanje svih faktora rizika, koje tim za upravljanje rizikom predloži, mogu se identifikovati dva skupa faktora rizika:

- *rizik sa najvećim uticajem*, tj. koji ozbiljno pogađa organizaciju i
- *rizik sa najvećim odnosom korist-rizik za napadača*, tj. onaj koji je ekstremno privlačan za napadača (gotovo bez rizika, a sa velikom dobiti).

Dakle, potrebno je dodati stohastičku dimenziju u oba seta. Baze podataka koje skupljaju informacije o kompjuterskim incidentima u svetu, mogu pomoći da se događaj rizika u organizaciji proceni sa većom verovatnoćom i da tim za UR bolje razlikuje verovatan rizik od mogućeg.

Dobar pristup proceni rizika je određivanje prioriteta za akciju tretmana rizika i troškove na bazi *Parteo principa* 80:20. U prvom koraki treba identifikovati i implementirati, kontrole za ublažavanje kritičnih faktora rizika, sa – (1) *najvećim uticajem, (2) najvećom verovatnoćom i (3) najvećim odnosom korist/rizik za napadača*, a, zatim, za one faktore rizika, koji imaju procenu *visok,* barem u dve od ove tri dimenzije.

Taksonomija rizika moguća je u odnosu na više kriterijuma. U odnosu na **oblast izlaganja**, riziku su izloženi: *ljudski faktor, tehnologija, okruženje i poslovni procesi.* U odnosu na **izvor** rizik može biti *operativni* – dolazi od funkcionisanja organizacije i *strateški* – dolazi od poslovnih, socijalnih, političkih, ekonomskih i tehnoloških faktora. Specijalni tip strateškog rizika je *rizik za ugled* organizacije, koji nastaje posle realizacije rizika

bilo kojeg tipa i prirode (primer je kompromitacija *web* servera banke). Alternativno, u odnosu na **izvor**, rizik se može podeliti na *hazardni* – od fizičkog okruženja i *finansijski* – od kredita, inflacije, tržišnih cena itd. U odnosu na **uticaj** rizik se može, sa dovoljnom tačnošću, rangirati u kvalitativnom pristupu sa: *visok, srednji, nizak,* a u kvantitativnom – izraziti u novčanim jedinicama očekivanih godišnjih gubitaka (OGG), koji bi nastali da nema kontrola za ublažavanje rizika.

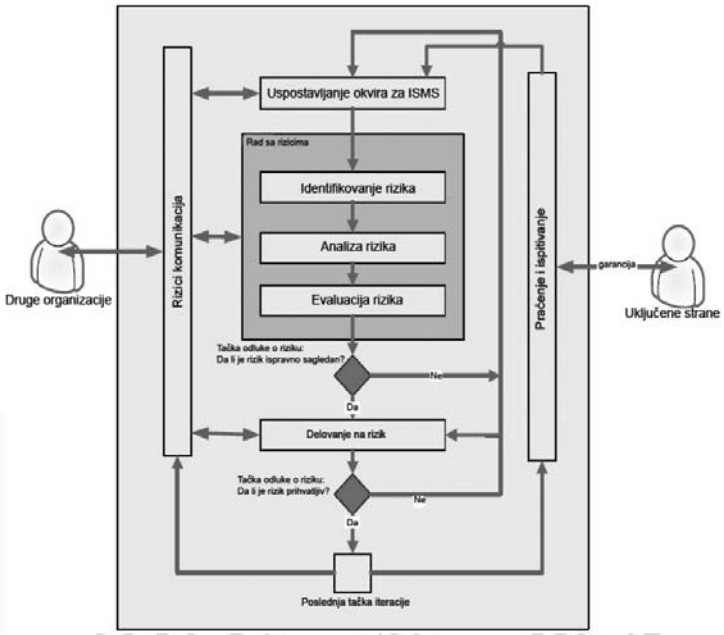
2.2.3.1. Uspostavljanje konteksta za procenu rizika

U standardu ISO/IEC 27005 proces *uspostavljanja konteksta* za procenu i analizu rizika odvija se kroz četiri faze:

1. definisanje osnovnih parametara za upravljanje rizikom;
2. definisanje obima i granica analize i procene rizika;
3. uspostavljanje i organizacija tima za upravljanje rizikom;
4. uspostavljanje strukture i procesa za procenu rizika.

1. Definisanje osnovnih parametara za upravljanje rizikom uključuje određivanje potencijalno raspoloživih resursa za analizu i procenu rizika:
   a. *izabrati odgovarajući pristup/metodologiju za procenu rizika* – ISO/IEC TR 13335-3, ISO/IEC 27005, NIST SP 800-30, CRAMM, OCTAVE, BAR itd., pomoćne alat za proračun faktora rizika (RA2, COBRA, HESTIA i dr.), uzorke radnih tabela i standardne taksonomije pretnji i ranjivosti;
   b. *definisati kriterijume za evaluaciju rizika* – legalne zahteve, ugovorne obaveze, operativne i poslovne gubitke i dr;
   c. *uspostaviti kriterijume za procenu uticaja rizika* – operativne, tehničke, finansijske, legalne, normativne, socijalne i dr;
   d. *uspostaviti kriterijume za prihvatanje rizika* – mogući su različiti nivoi praga prihvatanja rizika u istoj organizaciji;
   e. *definisati potencijalno raspoložive resurse* – za uspostavljanje tima za UR u organizaciji, izbor i implementaciju kontrola zaštite za tretman rizika.
2. Definisanje obima i granica analize i procene rizika može da uključi strateške i kratkoročne poslovne ciljeve, poslovne procese i strategiju razvoja, politiku zaštite organizacije, legalne i normativne zahteve, oblast primene i razloge za isključivanje nekog objekta iz procesa UR. *Granice* procesa UR tipično uključuju: *poslovne ciljeve i politiku, čistu informacionu imovinu, ljude, fizičko i socijalno–kulturološko okruženje i poslovne procese i aktivnosti.*
3. Uspostavljanje i organizacija tima za upravljanje rizikom uključuje identifikaciju i analizu relevantnih učesnika, izbor lidera i članova tima, definisanje uloga i odgovornosti svih učesnika i uspostavljanje zahtevanih odnosa i potpune komunikacije između tima i ostalih učesnika.

4. Uspostavljanje strukture procesa procene rizika uključuje *uspostavljanje konteksta za upravljanje rizikom, identifikovanje, analizu, evaluaciju i procenu rizika, tretman i prihvatanje preostalog rizika* (Sl. 2.6).



Sl. 2.6. Funkcionalni model procesa procene rizika

U procesu procene rizika zahteva se potpuna komunikacija, koja uključuju sakupljanje informacija za identifikaciju faktora rizika, analizu toka informacija za izbegavanje/redukciju rizika, konsultacije za relevantne učesnike, radi boljeg razumevanja procesa UR itd. Plan komunikacije treba razviti u ranoj fazi procesa.

Kvalitet procesa UR, skupljanje informacija o riziku i otpornost sistema zaštite na proboj, obezbeđuju se izradom procedure za UR. Glavni cilj izrade procedure za UR je da demonstrira generalni stav organizacije prema zaštiti i smanji uticaj proboja sistema zaštite na poslovne procese.

Nadzor, kontrola i revizija procesa UR identifikuju promene faktora rizika u ranoj fazi. Glavni cilj je odrediti relevantnost tekuće procene rizika i po potrebi preduzimati korektivne akcije, uključujući redefinisanje: *konteksta, kriterijuma za evaluaciju rizika, pristupa i metodologije za procenu rizika, opcija tretmana rizika, metoda komunikacije* itd. Predmet kontrole i revizije u procesu UR, mogu biti zakonski okvir, okruženje, konkurencija, kriterijumi za evaluaciju rizika, itd.

2.2.3.2. Proces analize i evaluacije rizika

Proces za procenu rizika obuhvata faze *analize* (identifikacije i estimacije) i *evaluacije* rizika.

Analiza rizika podrazumeva analizu svakog faktora rizika, u odnosu na to zašto i kako može nastati. Faktore rizika treba identifikovati, a zatim izvršiti estimaciju.

Identifikacija faktora rizika mora biti sveobuhvatna, struktuirana i argumentovana. Korisno je identifikovati faktore rizike koje treba tretirati pod kontrolom organizacije, ali i izvan te kontrole. Faktori rizika se mogu nalaziti u oblasti imovine **(A)**, kombinovanih pretnji (**∑T**) i ranjivosti (**V**), a identifikuju se u odnosu na *verovatnoću uticaja* ili da će pretnja/e iskoristiti ranjivost/i i naneti štetu. U ovoj fazi se definišu i neprihvatljive posledice uticaja faktora rizika, kao i primenljivi metodi za identifikaciju faktora rizika – *ček liste, intervjui, sistemska analiza i sistem inženjerske tehnike*. *Očekivani izlazi* iz ove faze procesa analize rizika su dokumenti: *inventar informacione imovine, taksonomija relevantnih pretnji i taksonomija relevantnih ranjivosti.*

Estimacije parametara rizika može biti kvantitativna ili kvalitativna statističko – numerička aproksimacija**.** Ova faza analize rizika uključuje sve faktore neodređenosti u proceni rizika (NIST SP 800-30). Faktori neodređenosti u proceni rizika mogu se smanjiti primenom formalnih modela i složenog matematičkog aparata, što je nerentabilno i praktično se retko koristi. Sasvim prihvatljiv metod redukcije faktora neodređenosti u proceni rizika je izbor najnepovoljnije estimacije, koja daje najveći rizik, čime se proaktivno utiče na izbor robustnijih kontrola zaštite za efektivniji tretman rizika. Na primer, parametri rizika (**A, T, V**), relativno nezavisnih objekata mogu se u estimaciji **Rr** množiti ili sabirati:

$$Rr = A \bullet V \bullet \sum T, \text{ ili } Rr = A + V + \sum T \qquad (3.1)$$

Množenjem parametara rizika umanjuju se posledice uticaja faktora neodređenosti na tačnosti procene rizika, pa je bolja aproksimacija od sabiranja parametara rizika.

Identifikacija i estimacija informacione imovine (**A**) obuhvata dve ključne kategorije – *listu invent*ara i *bezbednosnu kategorizaciju i klasifikaciju* imovine. Pod *inventarom informacione imovine* u standardu se podrazumevaju svi materijalni i nematerijalni objekti koji imaju neposredan i posredan značaj za bezbednost informacija. *Klasifikacija informacione imovine*, prema standardu ISO/IEC 27001, prepoznaje šest kategorija grupisanih u *čistu informacionu imovinu*, *fizičku imovinu* i *humanu imovinu*, ali ostavlja i mogućnost da organizacija uvede i nove kategorije ukoliko postoji potreba. U skladu sa obimom i nivoom procenjenog rizika, inventar imovine organizacije, treba srazmerno, ali ne previše detaljno, grupisati u *bezbednosne kategorije,* da bi se smanjila kompleksnost analize i procene rizika. Ovo je veoma značajna faza, jer predstavlja ulaz u proces analize rizika. Propusti u izradi ove liste mogu imati velike posledice, jer se neće tretirati kroz proces analize, procene i ublažavanja rizika.

Svi objekti **A** treba da imaju svoje *vlasnike* (staraoce), odnosno da za njih budu zaduženi neki entiteti organizacije. Vlasništvo nad informacijama mogu imati poslovni procesi, definisani skup aktivnosti, aplikacije, definisane grupe podataka i zaposleni. Rutinski poslovi sa vlasničkim informacijama ili objektima imovine mogu biti delegirani, ali odgovornost ostaje na vlasniku. Vlasnici koji su zaduženi za objekte A, odgovorni su za *klasifikaciju informacija* i *bezbednosnu kategorizaciju imovine*, određivanje i periodičnu proveru prava pristupa (ovlašćenja i privilegija).

Informacije mogu imati različite stepene osetljivosti i kritičnosti za poslovanje. Cilj klasifikovanja informacija je održavanje odgovarajućeg nivoa zaštite. Informacije treba klasifikovati po potrebi, prioritetima i očekivanoj poverljivosti prilikom upotrebe. Neke od njih zahtevaju posebne tretmane i stepene specijalne zaštite. Šema za klasifikovanje informacija treba da sadrži stepene osetljivosti i uputstva za upotrebu u zavisnosti od stepena osetljivosti. Odgovornost za klasifikaciju informacija snosi vlasnik. U praksi se najčešće uspostavlja nekoliko stepena klasifikacije informacija, na primer: *javne, interne, poverljive, strogo poverljive itd.* Klasifikacionu šemu i mere u odnosu na klasifikaciju svaka organizacija kreira prema svojim potrebama i mogućnostima. Bitno je napomenuti da je u praksi gotovo nemoguće naći organizaciju koja ima savršen sistem klasifikacije informacija, iz nekoliko razloga. Informacije se često ne klasifikuju, zaposleni se ne pridržavaju instrukcija i mera iz klasifikacione šeme ili se zahteva višekratna primena klasifikacije nad istom informacijom (što je najteže izvodljivo). Zatim, informacije tokom korišćenja učestvuju u procesima, mogu biti podložne promeni klasifikacije u odnosu na vremenski period (neke strogo poverljive, to više nisu posle određenog vremena), a često se ukazuje i potreba za promenom vlasnika informacije u procesu. Taj komplikovani proces nije uvek jednostavno ispratiti, pa sistem klasifikacije informacija uvek treba poboljšavati. Na ovaj proces se takođe može primeniti PDCA model, kao način poboljšanja sistema klasifikacije, što je sa aspekta ISMS *Demingov točak u točku.* Pravila upotrebe informacija i drugih objekata informacione imovine, treba da budu definisana, dokumentovana (kroz *politiku komponenti sistema zaštite*[31]) i implementirana. Svaku razvijenu politiku, u kontekstu ISMS, odobrava glavni menadžer, a odgovornost za sprovođenje snose izvršni menadžeri i zaposleni.

Za estimaciju vrednosti imovine (**A**) mogu se izabrati kvantitativne ili kvalitativne skale gradacije. *Kvantitativna skala gradacije* izražava se u novčanim jedinicama troškova nabavke, oporavka ili popravke posle nanete štete, što uvek nije dovoljno za sve objekte imovine. Kvantitativni metodi se uglavnom koriste u okruženjima sa rigoroznim zahtevima za procenu rizika (vojska, policija itd.).

Kvalitativna skala gradacije imovine može se kretati u različitim opsezima, npr. *zanemarljiv (Z), vrlo nizak (VN), nizak (N), srednji (S), visok (V), vrlo visok(VV), kritičan (K).* Kako se za bezbednosnu kategorizaciju imovine uzima najnepovoljniji slučaj, u praksi je dovoljna skala gradacije: **N, S, V.** Za pripisivanje vrednosti objektima **A**, mogu se koristiti brojni, nedvosmisleni i dokumentovani kriterijumi, što je i najteža faza ovog koraka,

31 NIST definiše politiku zaštite: *organizacije, IKTS, sistema zaštite (ISMS) i komponenti zaštite.*

kao što su: *originalna nabavna cena, troškovi zamene i/ili re-kreiranja u slučaju kvara/ destrukcije, troškovi nastali gubitkom CIA, gubitak ugleda, klijenata, konkurentske prednosti na tržištu i sl.* Takođe, mogu se koristiti i generički kriterijumi za estimaciju, kao što su: *povreda zakona i/ili normativa, neusaglašenost performansi poslovnih procesa, ugrožavanje privatnosti ličnih informacija i lične sigurnosti, negativan uticaj na primenu zakona, narušavanje javnog reda, ugrožavanje životne sredine itd.* Neki objekti A mogu imati više kriterijuma za pripisivanje vrednosti, na primer, *plan poslovanja* se može vrednovati na bazi *vrednosti razvoja i izrade plana* (Ap), *vrednosti unosa podataka u plan* (Ad) *i vrednosti plana za konkurenciju* (Ak).

Kvantitativna procena vrednosti imovine uključuje cenu nabavke, implementacije i održavanja. Sve vrednosti višestruke i kombinovane procene se maksimiziraju (prema kriterijumu bezbednosne kategorizacije – Bk). Konačna vrednost koja se dokumentuje mora biti pažljivo određena. Na kraju, sve estimacije vrednosti objekata A treba redukovati na zajedničkoj osnovi.

Vrednost **A** generalno se procenjuje na bazi *značaja* objekta informacione imovine za poslovanje organizacije, tako da najznačajniji (najkritičniji) objekti imaju najveću vrednost **A**. U objektnom pristupu, vrednost **A** se može odrediti *sabiranjem* relativno nezavisnih atributa kvaliteta imovine, koji aditivno doprinose njihovoj vrednosti za organizaciju:

$$\mathbf{A = P + R + I} \qquad \textbf{(3.2)}$$

gde je: **P** – *poverljivost,* **R** – *raspoloživost,* **I** – *integritet* objekta **A**.

Primer izbora kriterijuma za estimaciju težinskih faktora i proračun vrednosti **A,** koji se primenjuju na sve tri grane objekata za zaštitu (**P, R, I**), dat je u Tabela 2.2.

Tabela 2.2. Kriterijumi za određivanje težinskih faktora vrednosti A

Nivo vrednosti	Težinski faktor	Definicija – kriterijumi
Najveći	1	Ova imovina (**A)** ima najvišu vrednost za organizaciju i može se vrednovati i više od očekivane tržišne vrednosti. Gubitak može imati *ozbiljan uticaj na ukupno poslovanje*.
Srednje visok	2	Ova imovina ima vrlo visoku vrednost za procese rada, a gubitak može imati *ozbiljan uticaj na neke poslove*.
Srednji	3	Ova imovina je značajna i može biti zamenljiva, a gubitak može imati *trenutne, ozbiljne posledice za poslovanje*.
Srednje nizak	4	Ova imovina je zamenljiva, ali je cena zamene relativno visoka, pa može imati samo *umeren uticaj na ukupno poslovanje*.
Nizak	5	Ova imovina nema stvarnu ekonomsku vrednost unutar procesa rada i *može se lako i jeftino zameniti*.

Identifikacija i estimacija ranjivosti sistema (**V**) uključuje ranjivosti *organizacije, procesa i procedura, upravljanja, personala, fizičkog okruženja, arhitekture i konfiguracije IKTS, hardversko-softverske i komunikacione opreme*, odnosno, sve ono što napadač može iskoristiti za dobijanje određene prednosti u odnosu na A. Ranjivost IKTS je interno svojstvo, a odnosi se na greške softvera, hardvera i konfiguracije. Identifikuju se ranjivosti, koje procenjeni izvori pretnji mogu iskoristiti i naneti štetu imovini A i poslovnim procesima organizacije. *Postojanje ranjivosti samo po sebi ne nanosi štetu; potrebno je da postoji pretnja koja je može iskoristiti*. Ranjivost koja nema odgovarajuću pretnju i ne može se iskoristiti ne zahteva implementaciju kontrola zaštite, ali se mora prepoznati i monitorisati na promene. Ranjivost može biti i pogrešno implementirana ili nekorektno korišćena *kontrola zaštite*, ali i vezana za atribut objekta imovine, koji nije inherentno namenjen za korisničku upotrebu. Prema ISO/IEC 27005 uobičajena taksonomija ranjivosti IKTS je na *okruženje i infrastrukturu, hardver, softver, komunikacije, dokumentaciju, personal, procedure i opšte primenljive ranjivosti.*

Ranjivost informacione imovine (V) može se odrediti estimacijom više faktora koji utiču posredno ili neposredno na vrednost ovog parametra. Kako uticaj ovih relativno nezavisnih pojedinačnih faktora na vrednost V ima značajan stepen neodređenosti, ovi se faktori množe, što daje bolju aproksimaciju vrednosti V:

$$\mathbf{V = D \bullet K \bullet Tr \bullet Is \bullet Za} \qquad \mathbf{(3.3)}$$

gde su: **D** – *detektibilnost*, **K** – *korisnost*, **Tr** – *trajnost*, **Is** – *iskoristivost*, **Za –** *zaštićenost*.

Relevantni težinski faktori ranjivosti objekata **A** procenjuju se, sa aspekta agenta pretnje, u odnosu na atribute **D, K, Tr, Is** i **Za**. Težinske faktore treba procenjivati i računati za svaku poznatu tačku ranjivosti u odnosu na ove atribute. Primer estimacije **V** na osnovu pet navedenih atributa, poređanih po prioritetima od najznačajnijeg **(1)** do najmanje značajnog **(5),** dat je u Tabeli 2.3 [67, 35].

Tabela 2.3. Primer procene relevantnih faktora ranjivosti (V)

Atributi V	Procena ranjivosti (*V*)
(1) Vidljivost (D)	Verovatnoća da kompetentan agent pretnje postane svestan vrednosti informacije i da može pristupiti ovim informacijama.
(2) Korisnost (Ko)	Verovatnoća da agent pretnje uvidi korisnost informacije, da će informacija zadovoljiti neku zainteresovanu (konkurenciju).
(3) Trajnost (Tr)	Datum iza koga informacija više neće biti korisna napadaču i mogućnost korišćenja informacije pre toga datuma.
(4) Iskoristivost (Is)	Mogućnost upotrebe informacije u vreme i na način koji su kritični za vlasnika informacije.
(5) Zaštićenost (Za)	Dokumentovana politika zaštite i ograničen pristup informacijama, korisnici su potpisali NDA sporazum o neotkrivanju informacija.

Svakom odgovoru u Tabeli 2.3. pripisuje se jedan od ponuđenih težinskih faktora primenjene metrike (1–5; 1–10; *nizak, srednji, visok* itd.) onako kako ih procenjuju vlasnici objekata. Ranjivost objekata IKTS, često je teško procenjivati pre incidenta, jer, u suštini, najčešće napad potvrđuje da li postoji ranjivost. U ovom procesu pored liste pitanja za glavne atribute parametra ranjivosti u Tabeli 2.3, obavezno treba ispitati ranjivosti (nedostatak/neadekvatnost) *politike, standarda i procedura, obuke, definisanja uloga, odgovornosti, naloga i ovlašćenja, veliki broj pristupnih tačaka RM, mogućnost fizičkog pristupa serverima* i dr. U procesu estimacije, treba procenjivati ranjivosti po svim glavnim atributima za svaku tačku ranjivosti. Osnovni proaktivni metod za procenu ranjivosti IKTS podrazumeva testiranje i uključuje automatizovani alat za skeniranje ranjivosti (RS/RM), bezbednosno testiranje i evaluaciju – STE (*Security Testing and Evaluation*) i testiranje na proboj. Metod skeniranja je pouzdan za kontrolu ranjivosti, ali može proizvesti lažne pozitive. Proces STE efektivnosti kontrola zaštite u operativnom okruženju, vrši se u procesu sertifikacije i akreditacije sistema. Testiranje na proboj proverava mogućnost zaobilaženja kontrola zaštite, sa aspekta izvora pretnji (tzv. *etički hakiing*).

Identifikacija i estimacija pretnji (**T**) za *imovinu* **A** koriste neku od taksonomija pretnji. *Pretnja* implicira neku akciju, koja dolazi iz okruženja sistema, koji je predmet analize, tj. neki aktivni subjekt koji izvršava akciju prema IKTS. Standard ISO/IEC 27005 deli pretnje na *prirodne (**E**), humane (**H**), namerne (**D**) i slučajne (**A**).* Realna pretnja je najčešće *kombinacija* ovih izvora i *dinamički* se menja u vremenu. U kontekstu i obimu analize i procene rizika, treba identifikovati sve relevantne **T**. Za svaku individualnu pretnju treba *identifikovati izvor* i *proceniti verovatnoću realizacije* – frekvenciju pojave i intenzitet, a dovoljno je koristiti skalu gradacije **N, S, V**.

Ulazne veličine za procenu pretnji treba obezbediti od *vlasnika/korisnika imovine, odeljenja za upravljanje ljudskim resursima, izvršnih menadžera, IKT i specijalista, zaštite i dr.* kao i iz statističkih podataka i taksonomija pretnji. Upotreba taksonomije pretnji je korisna, ali treba uzimati u obzir dinamiku promena kombinovanih pretnji, zbog promena poslovanja, tehnologija, okruženja, malicioznih kodova itd. Primeri taksonomije bezbednosnih pretnji – stabla pretnji i skala gradacije za procenu pretnji, mogu se naći u standardima ISO/IEC 27005 i NIST SP 800-35.

Estimacija vrednosti parametra **T** u fazi analize rizika, daje najbolju aproksimaciju za procenu rizika, kao kombinacija dinamički promenljivih pretnji – **∑ T:**

$$T=T1+T2+...+T8=\sum T \tag{3.4}$$

Za analizu rizika prihvatljiva je taksonomija *kombinovanih pretnji* (**∑ T** *)* u odnosu na: (1) *posledice uticaja* (štetne **– Št,** neškodljive **– Nš)**, (2) *izvore nastanka* (iznutra – **Un,** spolja – **Va)** i (3) *način napada* (sofisticirane – **So,** nesofisticirane – **Ns),** koja daje ukupno $\mathbf{2^3=8}$ različitih kombinacija pretnji. Primeri za svaku od **osam** kombinovanih tipova pretnje dati su u Tabeli 2.4.

Tabela 2.4. Primeri tipova kombinovanih pretnji

Pretnja –T	Opis / primer
ŠtSoUn	Aktivnosti nezadovoljnog sistem administratora
ŠtNsUn,	Aktivnosti nezadovoljnog zaposlenog (ne-administratora)
NšSoUn	Aktivnosti znatiželjnog administratora (STE izveštaj poslednjih ranjivosti) Slučajno oštećenje od strane administratora (brisanje datoteke korisnika)
NšNsUn	Aktivnosti znatiželjnog korisnika (pogađanje lozinke) Slučajno oštećenje od strane znatiželjnog korisnika (brisanje datoteke)
ŠtSoVa	Industrijska špijunaža; aktivnosti veštog osvetoljubivog napadača
ŠtNsVa	Aktivnosti napadača ograničenih sposobnosti, ali jako zainteresovanih za specifične objekte (*e-mail spam ili trial-and-error* napadi)
NšSoVa	Aktivnosti veštog, odlučnog i znatiželjnog korisnika (čovek vs. mašina)
NšNsVa	Aktivnosti znatiželjnog korisnika ("šta/kako ovo radi?") Nenamerna aktivnost koja se može interpretirati kao maliciozna

Proračun težinskih faktora za verovatnoću pojave bezbednosnog incidenta potrebno je izvršiti za svaki objekat **A**. Iako svaka organizacija bira sama svoj sistem težinskih faktora (ponderisanja), moguća je primena sledećih kriterijuma (Tabela 2.5).

Tabela 2.5. Proračun težinskih faktora za verovatnoću pojave incidenta

Nivo	Težinski faktor	Definicija
Vrlo visok	1	Vrlo visoka verovatnoća događaja T, ako nema korektivne akcije
Visok	2	Visoka verovatnoća događaja T, ako nema korektivne akcije
Srednji	3	Pretnja ima umerenu verovatnoću događanja
Nizak	4	Smatra se da je rizik od događanja ove pretnje vrlo nizak
Vrlo nizak	5	Vrlo niska verovatnoća da će se ovaj incident dogoditi

Proračun težinskih faktora intenziteta potencijalnih pretnji potrebno je izvršiti za svaki objekat **A**. Iako svaka organizacija bira sama sistem ponderisanja, za ponderisanje intenziteta potencijalnih **T** korisni su sledeći kriterijumi (Tabela 2.6).

Tabela 2.6. Kriterijumi za ponderisanje intenziteta potencijalnih pretnji

Nivo uticaja	Težinski faktor	Definicija/posledice
Eliminiše	1	Incident potpuno uništava objekat A i organizacija se teško može oporaviti; incidenti su teški za kontrolu i zaštitu.
Razoran	2	Incidenti mogu biti razorni i bez neposrednog i adekvatnog odgovora potpuno uništiti objekte A; dovode do značajnih finansijskih gubitaka i gubitka javnog ugleda.
Kritičan	3	Incidenti od kojih se organizacija može oporaviti dobrim upravljanjem incidentom i implementacijom odgovarajućih kontrola zaštite; dovode do srednjih gubitaka i neprijatnosti.
Kontrolisan	4	Uticaj incidenta je kratkoročan i može se kontrolisati; uticaj mogu bit minorna neprijatnost i minimalni troškovi.
Iritirajući	5	Incidenti su obično beznačajni i izazivaju samo lokalnu iritaciju; mera-ma zaštite treba ih izbeći ili kontrolisati.

Generalno, *težinske faktore* izvora **T** treba kategorisati od najvećih do najmanjih, npr. pretnje od ljudi su teže od prirodnih događaja. *Proračun težinskih faktora frekvencije pojave **T***, potrebno je izvršiti za svaki objekat **A**. Iako svaka organizacija bira sistem ponderisanja, korisni su sledeći kriterijumi (Tabela 2.7):

Tabela 2.7. Kriterijumi za određivanje težinskih faktora frekvencije incidenta

Nivo	Težinski faktor	Definicija
Vrlo visok	1	Frekvencija incidenta je vrlo visoka i može biti razoran.
Visok	2	Frekvencija incidenta je visoka i može se ponoviti.
Srednji	3	Incident se može često dogoditi, ali normalno nije predvidiv.
Nizak	4	Incident ima nisku frekvenciju i nije ponovljiv, ne bi trebalo biti više od jednog incidenta u jednom radnom ciklusu.
Vrlo nizak	5	Ovaj incident se smatra vrlo retkim i periodičnim.

Za proračun se mogu koristiti i statistički elementi za alternativnu procenu verovatnoće incidenta za najveći broj tipova poznatih potencijalnih **T**, mereni verovatnoćom od **0 – 1** ili numeričkim, kvalitativnim težinskim faktorima od **0 – 5.**

Estimacija uticaja (**Ut**) je mera efekata i negativnih posledica, koje na imovinu **A**/ poslovanje, može izazvati neki napad. Uticaj je posledica verovatnoće da će neka pretnja/e iskoristiti neku/e ranjivost/i i naneti štetu imovini **A**, a može se ostvariti samo ako postoji [49]:

- *izvor slučajne pretnje*: događaj/incident unutar perimetra bezbednosnog rizika i ranjivosti, koju ta pretnja može iskoristiti i/ili
- *izvor namerne pretnje*: stimulacija napadača (motivacija, odlučnost, resursi, sposobnost, prilika), atraktivnost **A** i **V** koju **T** može iskoristiti.

Standard ISO/IEC 27005 razmatra samo *operativne*, a ne i *potencijalne* posledice uticaja. *Operativni uticaj* može biti direktan ili indirektan. Primer *direktnog* uticaja su troškovi za zamenu izgubljene imovine. *Indirektan* uticaj su troškovi prekida operacija, potencijalne zloupotrebe informacija, zbog proboja sistema zaštite, povrede normativa i etičkog kodeksa poslovanja itd.

Za kvantitativnu ili kvalitativnu estimaciju uticaja određuje se težinski faktor intenziteta **Ut** na pojedinačne objekte **A**. Glavna *prednost kvalitativne* analize **Ut** je u određivanju prioritetnih faktora rizika i zona ranjivosti, koje neposredno treba otklanjati. *Nedostatak kvalitativne* analize **Ut** rizika je u tome što ne obezbeđuje specifične kvantitativne mere i procenu odnosa troškovi-korist (*cost-benefit)* preporučenih kontrola zaštite. Glavna *prednost kvantitativnih* metoda analize **Ut** rizika je, što obezbeđuje merenje **Ut** i *cost–benefit* analizu preporučenih kontrola zaštite. Nedostatak oba metoda je *neodređenost* i česta potreba kvalitativne interpretacije rezultata, što zavisi od izbora opsega faktora ponderisanja.

Primer *kvalitativne* procene i određivanja težinskih faktora uticaja rizika, koji uključuje komponente *vrednosti objekata* – **A,** *intenziteta pretnje* **– Ti,** *frekvenciju pretnje* **– Tf i** *verovatnoću pretnje* **– Tv** prikazan je u Tabeli 2.8.

Tabela 2.8. Komponente za određivanje težinskih faktora uticaja rizika

Komponente uticaja rizika (Ut)	Težinski faktori
Vrednost objekta – **A**	1 – 5 (1 je najveći)
Intenzitet potencijalne pretnje – **Ti**	1 – 5 (1 je najveći)
Frekvencija potencijalne pretnje – **Tf**	1 – 5 (1 je najveći)
Verovatnoća pretnje – **Tv**	1 – 5 (1 je najveći)

Za proračun ukupnog težinskog faktora **Ut** rizika, potrebno je množiti komponente **Ut** jednu sa drugom, da bi se smanjio efekat neodređenosti na tačnost rezultata. Ako se uzme u obzir da frekvencija i intenzitet pretnji nisu relevantni, ako se pretnja ne dogodi, uticaj se približno određuje kao faktor množenja *vrednosti imovine* – **A** i *verovatnoće događaja pretnji* – **Tv**:

$$Ut = A \bullet Ti \bullet Tf \bullet Tv \approx A \bullet Tv \qquad (3.5)$$

Na sličan način se preostali relativni rizik može odrediti pojednostavljenom relacijom:

$$Rrp = A \bullet Pu_t \quad (3.6)$$

gde je **A** – vrednost imovine, a **Pu_t –** verovatnoća uticaja ili da će **∑T** iskoristiti **V**.

U ovoj estimaciji, što je *manji* rezultat, to je *veći uticaj* faktora rizika. *Najveći uticaj* faktora rizika u primeru iz T. 2.9 je **1**, a najmanji – **625.** Glavni menadžer određuje kriterijume *prihvatljivosti rizika* i prioritete ublažavanja, npr. svaki R< 50 - zahteva trenutno ispitivanje, 1 < R < 200 = **V**, 200 < R < 400 = **S** i 400 < R < 625 = **N** rizik.

Faza evaluacije faktora rizika je procena rizika na bazi strogo utvrđenih kriterijuma, predefinisanih u fazi *definisanja parametara za upravljanje rizikom*. Obuhvata aktivnosti kao što su: *priprema za izradu plana tretmana; razmatranje predefinisanih kriterijuma za evaluaciju, uključujući bezbednosne kriterijume; značaj poslovnog procesa kojeg podržava A; zahtevi menadžmenta za tretman; zahtevi za preduzimanje hitnih akcija; poređenje nivoa estimacije faktora rizika sa predefinisanim kriterijumima za evaluaciju (npr. rezultatima prethodne procene rizika) i rangiranje faktora rizika po prioritetu za tretman (ublažavanje)*.

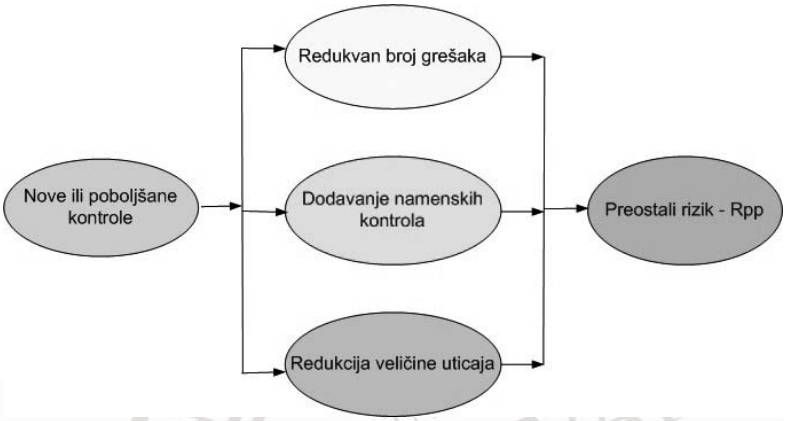
U ovoj fazi faktore rizika procenjene kao **N**, treba smatrati *prihvatljivim* i moguće je da menadžment/vlasnik sistema ne zahteva tretman ovih faktora rizika. Faktore rizika procenjene kao **S** i **V** treba tretirati, pri čemu faktore sa **V** – prioritetno.

Ukupan relativni rizik – **Rr** za imovinu **A**, određuje se na bazi evaluacije faktora rizika, kojih za neku prosečnu organizaciju, zavisno od dubine procene faktora rizika, kojih može biti i na hiljade. Grupišu se na prihvatljive (**P**) i neprihvatljive (**N**) faktore rizika. Kriterijume za **P** i **N** faktore rizika, predefinisane u fazi definisanja konteksta za procenu rizika, određuje menadžment, koji potpisivanjem **SOA** dokumenta definitivno prihvata predložene *kontrole zaštite* za tretman rizika i preostali relativni rizik (**Rpr)**. Očekivani izlazi iz faze evaluacije faktora rizika su prioriteti za tretman rizika: *lista prioriteta faktora neprihvatljivog rizika* i *lista prihvatljivih faktora rizika*.

Estimacija faktora preostalog rizika (Rrp), koji ostaje posle implementacije novih ili poboljšanih kontrola zaštite, znači da ni jedan IKTS nije sasvim oslobođen rizika i da sve implementirane kontrole ne eliminišu u potpunosti odnosne faktore rizika. Implementacija novih i poboljšanih kontrola može smanjiti rizik eliminisanjem nekih ranjivosti i smanjenjem negativnog uticaja. Kako je rizik identifikovan prema tipu specifičnih objekata i ranjivosti, sistem će imati jednu vrednost rizika po jednoj tački ranjivosti, koju pretnja iskoristi, a svaka ranjivost će imati jednu vrednost rizika po objektu na koji utiče. Ne postoji egzaktna matematička relacija za kvantitativan proračun **Rrp** za **A** u slučaju da **∑T** iskoriste **V,** sa implementiranim kontrolama zaštite (**KZ**) za ublažavanje rizika. Tako proces procene rizika daje dva rezultata – preostali relativni rizik bez učešća kontrola zaštite (**Rrp)** i prihvaćeni preostali rizik sa kontrolama zaštite **(Rpp)**. Nivo **Rpp** se približno računa iz jednačine [35, 67]:

$$Rpp = (Rrp/Kz) = (A \bullet Pu_t)/Kz \quad (3.7)$$

Uticaj pretnje na sistem raste sa porastom vrednosti **A, ∑T** i **V** i direktno povećava **Rpp**, dok **KZ** smanjuju nivo **Rpp**. Model proračuna **Rpp** dat je na Sl. 2.7.



Sl. 2.7. Implementirane kontrole zaštite i preostali rizik – Rrp

Posle implementacije kontrola zaštite za ublažavanje rizika, efektivnost uvođenja kontrola zaštite **(Ekz)** može se proračunati formulom:

$$Ekz = (Rpr–Rpp)/Rpr \quad (3.8)$$

Detaljna procena faktora rizika je kamen temeljac razvoja rentabilnog programa i plana zaštite. U plan zaštite korisno je ubaciti *kvantitativne parametre* – ukupne troškove zaštite, koji na preostalom nivou rizika (**Rpr**) treba da budu optimalni, odnosno, jednaki ili manji od procene ukupno očekivanih godišnjih gubitaka – **OGG**, koji mogu nastati ako se ne primene predviđene mere zaštite (**KZ)**. **OGG** treba da budu manji od **Rpr,** izraženog u novčanoj vrednosti. Ovakva vrednost **Rpr**, najčešće se predlaže menadžmentu, kao vrednost **Rpp** kod potpisivanja SOA dokumenta. Kako je vrednost **OGG** jednaka vrednosti $\mathbf{Pu_t}$ izraženog u novčanim jedinicama, **OGG** se mogu proceniti relacijom [67]:

$$\mathbf{OGG = Pu_t \times Ar} \quad \mathbf{(3.9)}$$

gde je $\mathbf{Pu_t}$ – verovatnoća da će se neka pretnja materijalizovati u datoj godini i uticati na imovinu **A**, a **Ar** – relativna vrednost imovine **A** na koju se pretnja odnosi.

Primer: *LAN ima 20 PC po ceni od 540 Eu po komadu. Očekuju se po jedan potpuni prekid rada, upad u sistem i krađa podataka godišnje (Pt=1). Primenom formule (3.9) biće:* ***OGG****= 1x (20 x 540) =* ***10.800 Eu****, pa su sve primenjene kontrole zaštite za sprečavanje ove procenjene štete rentabilne, ako im cena ne prelazi OGG*.

U praksi zaštite retko se koristi kompletna formalna metodologija za analizu i procenu rizika. Razvijeni su i skraćeni metodi za analizi rizika (OCTAVE, BAR), koji su praktičniji i brže dovode do prihvatljivih rezultata [9, 46,55].

2.2.3.3. Metodi procena ukupnog bezbednosnog rizika

Rezultati procene rizika koriste se za izbor kontrola za tretman rizika i dokumentuju u *politici zaštite* i *planu tretmana rizika.* Generalno, za identifikaciju rizika, u fazi procene, mogu se koristiti različite tehnike: *brainstorming* ili *brza analiza rizika* (BAR); *upitnik ili izjava o osetljivosti (IoO); identifikovanje poslovnih procesa i opis internih/eksternih faktora koji mogu uticati na ove procese; industrijski benchmarking; analiza scenarija napada (incidenata); generička procena rizika; ispitivanje incidenata; revizija (audit) sistema zaštite, studija HAZOP (hazard & operativnost)* itd**.**

Za generičku procenu opšteg *operativnog rizika* razvijene se tri ključne metodologije: (1) *procene rizika odozdo nagore, (2) sveobuhvatne analize i procene rizika i (3) procene rizika odozgo nadole*.

Procena rizika odozdo nagore uključuje istraživanje tržišta, predviđanje trenda, istraživanje i razvoj i analizu uticaja na poslovanje. Sveobuhvatna analiza rizika uključuje brojne faze i aktivnosti kao što su: modelovanje zavisnosti, SWOT analiza (snage, slabosti, prilike, pretnje), analiza drveta pretnji, planiranje kontinuiteta poslovanja (BCP), BPEST (biznis, politička, ekonomska, socijalna, tehnološka) analiza, modelovanje realnih opcija, odlučivanje na bazi stanja rizika i faktora neodređenosti, statističke implikacije, merenja glavnog trenda i faktora neodređenosti, PESTLE (Političko ekonomsko socijalno, tehničko i legalno) okruženje i dr. Procena rizika odozgo nadole uključuje tri glavne tehnike: analizu pretnji, analizu drveta grešaka i FMEA (Failure Mode&Effect Analysis) analizu [24].

Standard ISO/IEC 27005 diferencira i opisuje četiri osnovna metoda za estimaciju ukupnog rizika, koja se u osnovi zasnivaju na generičkoj metodologiji, ali imaju različite fokuse na parametre rizika i primenjuju različite vrste estimacije [24]:

1. metod matrice rizika sa predefinisanim vrednostima (ISO/IEC 13335-3);

2. metod merenja rizika rangiranjem ***T*** *prema rezultatima procene rizika;*

3. metod procene verovatnoće uticaja i mogućih posledica i

4. metod distinkcije između prihvatljivog i neprihvatljivog rizika.

Izlaz procene rizika je *Izjava o primenljivosti kontrola zaštite* (**SOA**) za ublažavanje rizika do prihvatljivog nivoa. Komercijalno su dostupne brojni interaktivni metodi i alati za procenu bezbednosnog rizika za informacionu imovinu. CRAMM metod je razvila engleska vladina agencija i koristi ga više od 40 država na najvišem nivou. Metod je skup, kompleksan za primenu, ali detaljan i pouzdan [9]. OCTAVE metod procenjuje faktore rizika za kritične objekte A i poslovanje organizacije. Metod je samonavodeći, sveobuhvatan, sistematičan i adaptivan i ne zahteva specijalistička znanja [46]. Za inicijalnu procenu rizika, dok organizacija nema kompletiran inventar A, koristan je metod brze analize rizika (BAR), koji zahteva aktivno angažovanje menadžmenta i praktičara poslovnih procesa [55].

2.3. REZIME

Upravljanje rizikom je *proaktivno* upravljanje sistemom zaštite. Procena rizika je metod za planiranje zaštite. Stohastička priroda pretnji, ranjivosti i uticaja otežava korišćenje analitičkih metoda u procesu analize i procene rizika. Drugi problem su *kvalitativna* i *kvantitativna* identifikacija i vrednovanje objekata imovine A, gde su podaci i informacije najznačajnije vrednosti. *„Vrednost"* imovine A može se dobiti samo indirektnim putem korišćenjem faktora *„uticaja"* pretnji na ranjive tačke sistema. Nemoguće je proceniti ove efekte bez specifičnog scenarija, a još teže napraviti evaluaciju materijalnih troškova gubitaka.

Dinamička „dimenzija" analize rizika je važna, jer se pretnje i iskoristive ranjivosti uvek menjaju. Ovo znači da se i nivoi zaštite moraju menjati tako da kompenzuju ove promene. Faktor promenljivosti se unosi u unutrašnje i spoljno okruženje, pa je za upravljanje promenama potrebno neprekidno skeniranje specifičnih događaja u okruženju. Promene u sistemu mogu izazvati interni događaji (nove aplikacije, novi zaposleni i sl.) ili promene u životnom ciklusu sistema (revizija zahteva i dizajna, implementacija sistema, monitoring i periodična kontrola itd.).

Brojni metodi kvantitativne analize rizika imaju prednosti, jer svode svaku analizu na novčanu vrednost. *Kvantitativna* analiza rizika ima problem memorisanja i akvizicije podataka. Za zaštitu nacionalnih interesa ili konkurentnosti na tržištu, češće se primenjuju *kvalitativni* metodi procene gubitaka umesto novčanih vrednosti. Generička metodologija procene rizika uključuje parametre vrednosti imovine (A), ranjivosti (V), pretnji (T), uticaja (Ut) ili da će pretnje iskoristiti ranjivosti i naneti štetu imovini i poslovnim procesima. Faktori neodređenosti koje u procenu rizika unosi stohastička priroda T i V, kompenzuju se množenjem parametara rizika, čime se dobije veći procenjeni rizik i implementira bolja zaštita.

Procenu rizika mogu pomoći brojne taksonomije T i V uz obavezno prilagođavanje kontekstu i okruženju. Na principima generičke metodologije, razvijena su četiri metoda sa različitim težištima u proceni ukupnog rizika (ISO/IEC 27005): *metod matrice rizika sa*

predefinisanim vrednostima (ISO/IEC 13335-3), metod merenja rizika rangiranjem pretnji prema rezultatima procene rizika, metod procene verovatnoće uticaja i mogućih posledica i metod distinkcije između prihvatljivog i neprihvatljivog rizika. Takođe, na raspolaganju su brojni pomoćni, interaktivni alati za procenu bezbednosnog rizika, kao što su aplikacije tipa COBRA, HESTIA, RA2 itd. Dobar interaktivni, kvalitativni metod za analizu rizika je CRAMM, kojeg koristi više od 40 zemalja u svetu za državne potrebe. Primena metoda nije jednostavna i zahteva dobru obuku analitičara. Metod OCTAVE je evaluacija faktora rizika za kritične objekte imovine organizacije. Metod je samonavodeći, sveobuhvatan, sistematičan i prilagođava se promenama realne situacije. Omogućava svim zaposlenim na svim nivoima organizacije da rade zajedno na identifikaciji i razumevanju faktora rizika i da donesu pravilne odluke za smanjenje rizika. Metod brze analize rizika (BAR) omogućava brzu i efektivnu analizu glavnih faktora rizika, sa uključivanjem kapaciteta organizacije i bez potrebe posebnog angažovanja specijalista za analizu rizika.

2.4. KLJUČNI TERMINI

Agent pretnje: entiteti (lice, organizacija, program) sposobni da namerno ili nenamerno pokrenu neki događaj, iskoristite ranjivosti sistema i nanesu štetu.

Analiza rizika: analiza vrednosti imovine, ranjivosti sistema, potencijalnih pretnji, i verovatnoće uticaja na objekte sistema i poslove organizacije.

Napad: realizovana pretnja koja ima potencijal da kompromituje sistem zaštite.

OGG: očekivani godišnji gubici koji mogu nastati, ako se sistem zaštite ne primeni**.**

Posledica: rezultat realizacije uticaja agenta pretnje, koji se izražava uglavnom u neželjenim promenama stanja sistema IKTS zaštite; sinonimi: *uticaj i šteta*.

Procena pretnje: analiza, identifikacija, estimacija i evaluacija *kapaciteta* agenta pretnje (resursa, motivacije, namere, sposobnosti i prilike).

Procena rizika: analiza verovatnoće da će ranjivosti sistema biti iskorišćene od potencijalnih pretnji i da će nastale posledice naneti štetu

Ranjivost: karakteristika sistema (kvar, ljudski faktori…) koja dopušta da se pretnja realizuje.

Resursi agenta pretnje: oprema, novac, znanje, veštine, motivacija itd. koji su na raspolaganju agentu pretnje da inicira napad.

Rizik: mera verovatnoće da će posledice nekog događaja kompromitovati objekte IKTS i naneti štetu organizaciji.

Scenario pretnje: specifičan agent pretnje koji preduzima specifičan tip napada u pokušaju da kompromituje (na jedan ili više načina) jedan ili više objekata IKTS.

Sredstva napada: mehanizam/medijum kojeg koristi agent pretnje za napad.

Uticaj: mera stepena oštećenja/promene uzrokovane nekom posledicom napada.

Vrednost objekata informacione imovine: mera ili izjava o značaju (osetljivosti) nekih objekata IKTS (ili alternativno cene), ako su isti kompromitovani; može se meriti kvantitativnim/kvalitativnim metodama; značaj ili cena su zavisni od potreba organizacije pa *vrednost* nije nužno objektivan pojam.

2.5. PITANJA ZA PONAVLJANJE

1. Generički okvir upravljanja rizikom sadrži sledeće korake:
   a. kategorizacija IKTS, planiranje, implementacija i procena *kontrola* zaštite, akreditacija IKTS, nadzor i revizija
   b. kategorizacija IKTS, izbor, implementacija, evaluacija, sertifikacija i revizija *kontrola* zaštite
   c. bezbednosna kategorizacija IKTS, izbor, implementacija i procena *kontrola* zaštite, akreditacija IKTS, nadzor i kontrola
2. Opšti model za procenu rizika sadrži sledeće konceptualne oblasti:
   a. plan upravljanja rizikom
   b. identifikacija ranjivosti
   c. analiza i procena rizika
   d. neodređenost koja interaktivno deluje sa faktorima procene rizika
   e. izbor i implementacijU *kontrola* zaštite
3. Hijerarhijski pristup upravljanju rizikom uključuje sledeće nivoe:
   a. uprave, poslovnih procesa, IKTS
   b. organizacije, poslovnih procesa, IKTS
   c. organizacije, IKTS, sistema zaštite
   d. organizacije, poslovnih procesa, IKTS, sistema zaštite
4. Generički metod kvalitativne procene bezbednosnog rizika procenjuje vrednosti:
   a. informacione imovine (A), napada (N), konfiguracije (K) i uticaja (U)
   b. informacione imovine (A), pretnji (T), ranjivosti (V) i uticaj (U)
   c. imovine IKTS (A), pretnji (T), ranjivosti softvera (V), rizika (R) i efektivnosti kontrola zaštite (Ekz)
   d. informacione imovine (A), pretnji (T), ranjivosti (V), uticaj (U) i rizika (R)

5. *Taksonomija rizika* je moguća u odnosu na više kriterijuma. Povežite *kriterijume* sa *tipovima* (atributa, faktora rizika, gubitaka):

Kriterijum	Tip (atribut rizika, gubitaka)
1. oblast izlaganja	a. *kvantitativni (OGG)* b. *okruženje* c. *tehnologija* d. *kvalitativni (nizak, srednji, visok; 1,2,3,4,5)* e. *operativni (hazardni, finansijski)* f. *strateški (rizik za ugled)* g. *poslovni procesi* h. *ljudski faktor*
2. izvor rizika	
3. uticaj	

6. Ublažavanje rizika od napada pomoću tehničkih sredstava može biti efikasno u određenim uslovima. Povežite te uslove sa merama zaštite:

Uslovi napada	Mera zaštite
1. Napad postoji 2. Iskoristiv Napad (postoji V) 3. Troškovi napada manji od dobiti 4. Gubitak je suviše velik	a. primeniti principe projektovanja, arhitekture, ne–tehničke i tehničke zaštite za ograničenje nivoa napada, a time i smanjenje gubitaka, npr. izborom netehničkih mera kao što je ograničavanje obima osetljivih procesiranih informacija
	b. primeniti zaštitu da se povećaju troškovi napada ili značajno smanjiti potencijalnu dobit napadača, npr. izborom ne-tehničkih mera kao što je ograničavanje obima osetljivih procesiranih informacija
	c. primeniti slojevitu zaštitu i projektovati arhitekturu sistema da se spreči iskorišćenje ranjivosti
	d. implementirati pouzdane tehnike za smanjenje verovatnoće neželjenog napada

7. Navedite osnovne korake formalne metodologije za uspostavljanje konteksta za procenu i analizu rizika:
   a. definisanje osnovnih parametara za upravljanje rizikom
   b. definisanje obima i granica analize i procene rizika
   c. definisanje programa zaštite
   d. uspostavljanje i organizacija tima za procenu rizika
   e. izrada plana i politike zaštite
   f. uspostavljanje strukture i procesa za analizu i procenu rizika
8. Kriterijumi za prihvatanje rizika se definišu u fazi:
   a. definisanja obima i granica analize i procene rizika
   b. definisanja osnovnih parametara za upravljanje rizikom
   c. izrade politike zaštite
   d. uspostavljanja i organizacija tima za procenu rizika
   e. uspostavljanja strukture i procesa za analizu i procenu rizika
9. Navedite opšte metode primene procesa tretmana rizika:
   a. metod matrice rizika sa predefinisanim vrednostima (ISO/IEC 13335–3)
   b. metod procene rizika odozgo nadole
   c. metod procene verovatnoće uticaja i mogućih posledica
   d. metod procene verovatnoće događaja pretnje
   e. metod distinkcije između prihvatljivog i neprihvatljivog rizika
10. Navedite redosled izvršavanja glavnih koraka procesa analize i procene rizika:
    a. procena V, procena A, procena T, procena Rr, implementacija k/z, izbor k/z za ublažavanje rizika, prihvatanje Rrp
    b. procena A, procena V, procena T, procena Rr, izbor k/z za ublažavanje rizika, implementacija k/z, prihvatanje Rrp
    c. procena T, procena V, procena A, izbor k/z za ublažavanje rizika, implementacija k/z, prihvatanje Rrp
11. *Pareto* princip u procesu upravljanja rizikom je poznat kao:
    a. pravilo 60:40
    b. pravilo 50:50
    c. pravilo 80:20
    d. pravilo 70:30
12. Formula za proračun *preostalog prihvatljivog rizika*–Rpp, približno glasi:
    a. Rpp= ((AxVx ∑T)/Kz) x Ut
    b. Rpp= (AxVx ∑T) x Ut
    c. Rpp= ((AxVx ∑T)/Kz)
13. U proceni rizika za određivanje vrednosti A obično je odgovoran i mora učestvovati:
    a. glavni menadžer organizacije
    b. specijalista zaštite
    c. pravnik organizacije
    d. digitalni forenzičar
14. Inventar imovine i taksonomije relevantnih pretnji i ranjivosti su izlazi iz procesa:
    a. uspostavljanja okvira za ISMS
    b. identifikovanja rizika
    c. estimacije rizika
    d. analize rizika
    e. evaluacije rizika
    f. ublažavanja (delovanja na) rizika
    g. prihvatanja rizika
15. Faktori neodređenosti rizika se uključuju u fazi:
    a. uspostavljanja okvira za ISMS
    b. identifikovanja rizika
    c. estimacije rizika
    d. analize rizika
    e. evaluacije rizika
    f. ublažavanja (tretmana) rizika
    g. prihvatanja rizika
16. U fazi procene ranjivosti (V), testiranje na proboj:
    a. proverava ranjivost mrežnih programa

b. proverava mogućnost zaobilaženja kontrola zaštite sa aspekta izvora napada
c. proverava ranjivost TCP/IP protokola
d. naziva se hakerski napad
e. naziva se etički haking

17. Standard ISO/IEC 27005 deli pretnje na:
    a. vanredne događaje (VD), ljudske greške (HG), kompjuterske incidente (KI) i hakerske napade (HN)
    b. prirodne (E), humane (H), namerne (D), slučajne (A*)* i kombinovane (K)
    c. prirodne (P), greške (G) slučajne (S) i namerne (N)
18. Faza evaluacije faktora rizika obuhvata sledeće aktivnosti:
    a. priprema za izradu plana tretmana rizika
    b. razmatranje kriterijuma za evaluaciju
    c. rangiranje kontrola zaštite za tretman rizika
    d. značaj poslovnog procesa kojeg podržava imovina A
    e. rangiranje faktora rizika po prioritetu za tretman rizika
    f. značaj procesa zaštite imovine A
    g. poređenje nivoa estimacije faktora rizika sa predefinisanim kriterijumima za evaluaciju
19. Standard ISO/IEC 27001 klasifikuje informacionu imovinu u:
    a. informacije, podatke, hardver, softver, mrežna infrastruktura
    b. informacije, računarske sisteme, računarske mreže, korisnike (ljude)
    c. čistu informacionu imovinu, fizičku imovinu, humanu imovinu
20. Najznačajniji izlaz iz procene rizika je dokument:
    a. plan tretmana rizika
    b. lista prioriteta prihvatljivog rizika
    c. lista prioriteta neprihvatljivog rizika
    d. izjava o primenljivosti kontrola zaštite (SOA)

3. UPRAVLJANJE PROGRAMOM ZAŠTITE INFORMACIJA

Po završetku ovog poglavlja razumećete:

- generičku strukturu dokumenta Program zaštite
- obim i strukturu Politika zaštite (organizacije, IS, ...)
- obim i strukturu Procedura zaštite
- obim i strukturu Plana zaštite
- značaj dokumentacije zaštite u sistemu zaštite
- koncept upravljačkog okvira
- koncept razvoja politike i procedure zaštite

3.1. UVOD

Program zaštite organizacije obuhvata *sve* što neka organizacija čini da proizvede, primeni, održava i unapredi bezbednost IKTS. Metodološka osnova za razvoj i uspostavljanje programa zaštite obično je u formi dokumentacije (zakoni, standardi, plan, politika itd.). Uspeh programa zaštite zavisi od tri kritična faktora uspeha – *procene rizika, dokumentacije i korisničke prihvatljivosti*. Program zaštite treba da sadrži najmanje *politiku, procedure, plan i uputstva za zaštitu*, kao i izjavu kojom se obavezuju odgovorna lica na izradu svih internih dokumenata zaštite.

Politika zaštite uspostavlja smernice, obezbeđuje resurse za zaštitu i treba da ima standardnu strukturu. Ključni je dokument programa zaštite i sadrži bezbednosne ciljeve, izražene kroz skup izjava o tome *ŠTA* treba raditi u oblasti zaštite. *Procedure* zaštite detaljno opisuju i dokumentuju procese zaštite i definišu *KAKO* nešto treba uraditi u skladu sa politikom. *Plan zaštite* detaljno specificira tehničko rešenje i proceduralne kontrole sistema zaštite, a *uputstva* objašnjavaju specifične aktivnosti u procesima zaštite. Najbitniji *zahtevi* za izradu, korisničku prihvatljivost i nametanje politike i procedura zaštite su: *jasno razumevanje vizije i ciljeva zaštite od strane menadžera; uključivanje specijalista zaštite, informatičara i što je moguće više predstavnika organizacionih jedinica; jasna artikulacija politike i procedura na koncizan i praktičan način i da reflektuju potrebe organizacije.* Menadžment obezbeđuje implementaciju i podstiče sprovođenje politike zaštite, koja se može izraditi u okviru jedinstvenog dokumenta ili kao skup samostalnih dokumenta (*politika*) na različitim nivoima.

3.2. RAZVOJ I STRUKTURA PROGRAMA, PLANA I POLITIKE ZAŠTITE

3.2.1. Struktura programske politike zaštite

Program zaštite se obično dokumentuje kroz kratku *Programsku politiku* zaštite IKTS, koja uspostavlja smernice za zaštitu, obezbeđuje resurse za implementaciju i treba da obuhvati najmanje sledeće komponente [55, 35, 41, 44, 55, 51]:

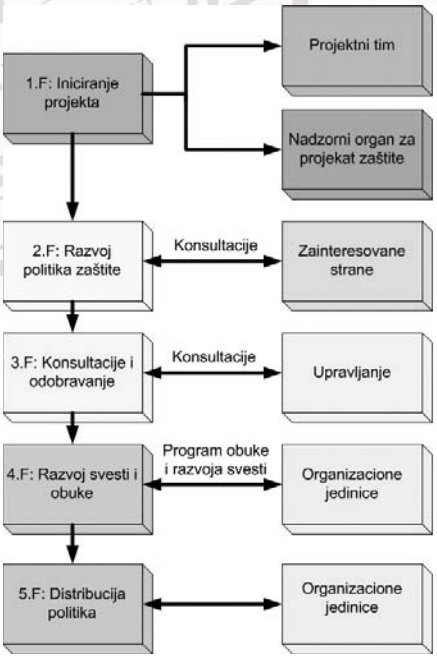
- *smernice menadžmenta,* koje ukazuju na pravac poslovanja, ciljeve zaštite i razloge uspostavljanja programa za zaštitu CIA informacija;
- *eksplicitnu podršku menadžmenta* za sve ciljeve zaštite informacija sa jasno određenim *objektima i granicama zaštite* informacione imovine;
- *odgovornost menadžmenta,* kojom se eksplicitno ističe strateška odluka za upravljanje programom zaštite;
- *odobrenje glavnog menadžera* sa zahtevom za *opštu usaglašenost* programa zaštite sa normativima i *specifičnu* – prakse sa politikom zaštite;
- *obavezu nametanja politike i sankcionisanja* za svaku neusaglašenost;
- *potpunu komunikaciju* svih zaposlenih sa menadžmentom.

Program zaštita treba da sadrži izjavu kojom se obavezuju odgovorna lica na izradu dokumenata zaštite (*plan, politiku, procedure* i *uputstva zaštite* [1, 6, 63].

3.2.2. Razvoj i struktura plana zaštite

Neki standardi (npr. NIST) *plan zaštite,* koji implementira *politike* i *procedure,* smatraju ključnim dokumentom programa zaštite. Generički proces razvoja plana zaštite obuhvata pet osnovnih faza [44]: *iniciranje projekta, razvoj politike zaštite, konsultacije i odobrenja, razvoj svesti i obuka i distribucija politike zaštite* (Sl. 3.1).

Takođe, neki autori mešaju *programsku politiku* i *plan zaštite*. Da bi se to izbeglo, pod *planom zaštite* treba podrazumevati *plan projekta*



Sl. 3.1. Generički proces razvoja plana zaštite

za razvoj i implementaciju politike i procedura zaštite. *Plan zaštite* mora biti usaglašen sa zakonskim propisima, poslovnim ciljevima, planom poslovanja i razvoja organizacije, politikom i procedurama zaštite i sa arhitekturom IKTS. Osnovna *struktura plana zaštite* može imati generičku formu tipičnog poslovnog plana, ali svaki mora biti specifičan za poslovne procese, kulturu rada, životni ciklus informacija, zakonske i ugovorne obaveze i raspoloživu tehnologiju za zaštitu. Uzorci za izradu plana zaštite su brojni (Internet, standardi zaštite), ali se konkretan plan zaštite smatra autorskim delom, predstavlja poverljiv dokument i retko se može naći objavljen. Generička struktura svakog plana zaštite treba da sadrži dve ključne komponente: u*loge i odgovornosti i upravljanje promenama* - plan kontrola ili plan tehničkog rešenja zaštite [1, 44].

3.2.2.1. Uloge i odgovornosti

Uloge i odgovornosti u sistemu zaštite, definišu se na bazi GAISP principa zaštite i pripisuju *glavnom menadžeru, izvršnim menadžerima i svim zaposlenim* [41, 44, 1].

Uloga glavnog menadžera je da obezbedi superviziju, definiše i upravlja glavnim smernicama programske i ISMS politike zaštite, nadzire i kontroliše realizaciju plana zaštite. U skladu sa zakonima za zaštite informacija u većini država, dve glavne odgovornosti su uvođenje standarda najbolje prakse zaštite i angažovanje odgovornih, stručnih i iskusnih lica na poslovima zaštite. Ova *odgovornost mora biti eksplicitno izražena* u programskoj politici zaštite.

Uloga glavnog menadžera uključuje sprovođenje GAISP principa i najbolje prakse zaštite i može se definisati kroz deset preporuka, i to za:

1. *program zaštite,* gde eksplicitno ispoljava liderstvo, finansijski obezbeđuje, kreira, nameće i regularno kontroliše sve aktivnosti;
2. *politiku zaštite*, gde obezbeđuje razvoj, implementaciju, kontrolu i primenu politike u skladu sa standardima, principima i najboljom praksom zaštite;
3. *upravljanje rizikom,* kroz redovnu reviziju procene, sa ciljem da identifikuje kritične objekte, pretnje i ranjivosti sistema i odobri plan ublažavanja rizika;
4. *projektovanje arhitekture sistema zaštite* tako što obezbedi, da arhitektura sistema zaštite podržava poslovne ciljeve organizacije;
5. *korisnike sistema,* gde su odgovorni za obuku i sve akcije legalnih učesnika i implementaciju politike i procedura zaštite;
6. *funkcionalnu pouzdanost IKTS,* kroz uspostavljanje niza kontrola pristupa objektima IKTS i regularnu verifikaciju integriteta programa;
7. *autentifikaciju i autorizaciju,* sa resursima za implementaciju i održavanje mehanizama za autentifikaciju i autorizaciju pristupa objektima IKTS;
8. *nadzor, kontrolu i reviziju* gde uspostavlja kapacitete za nadzor, kontrolu i reviziju i alate za merenje usklađenosti sa politikom zaštite;

9. *fizičku i personalnu zaštitu*, gde obezbeđuje kontrolu fizičkog pristupa objektima IKTS i bezbednosnu proveru zaposlenih u zaštiti;
10. *planiranje kontinuiteta poslovanja i oporavka sistema,* gde obezbeđuje razvoj i verifikaciju plana, periodično i regularno testiranje i efikasnu primenu.

3.2.2.2. Upravljanje promenama

Upravljanje promenama definiše se kao sistemsko uvođenje promena u *operativnom okruženju, tehnologijama, programima, hardveru, konfiguraciji RS/RM, radnom prostoru, zaposlenom personalu, rutinskim poslovima, tehničkim operacijama* itd. Za upravljanje promenama primenjuje se *opšta procedura* sa sledećom strukturom: *uvođenje promena, kataloška registracija, planiranje redosleda, implementacija i izveštavanje o izvedenim promenama*. Za svaku komponentu plana zaštite, treba zadužiti po jedno lice da upravlja promenama u skladu sa politikom zaštite [41].

Detaljan *plan zaštite* može se razviti za implementaciju politike zaštite*,* kada menadžment organizacije prihvati skup kontrola zaštite za ublažavanje rizika (SOA). Među ključnim faktorima uspeha implementacije plana zaštite su: *potpuna podrška menadžmenta; upoznavanje svih zaposlenih sa ciljevima zaštite; prepoznavanje jedinstvenih kulturoloških, etičkih i drugih zahteva organizacije; uključivanje kompetentnih i stručnih timova organizacije; imenovanje odgovornog tima ili pojedinaca za poslove zaštite; ugradnja mehanizama za detekciju, korekciju i do–obuku i ponovnu edukaciju u slučaju proboja sistema zaštite.*

3.2.3. Razvoj i struktura politike i procedura zaštite

Politika zaštite, ključni dokument programa i plana zaštite, sadrži bezbednosne ciljeve, koji podržavaju poslovne ciljeve organizacije i izjave na visokom nivou apstrakcije, koje govore *šta treba raditi* u oblasti zaštite; obezbeđuje okvir očekivanog i obaveznog ponašanja menadžera, zaposlenih, tehnologija i procesa; utvrđuje ciljeve, očekivanja i verifikovane korisničke zahteve, a koristi principe, instrukcije, procedure i smernice, koje su obavezne za organizaciju. *Sistem upravljanja zaštitom informacija* (ISMS) zahteva artikulaciju u dokumentovanoj *ISMS politici*, koja ima nekoliko funkcija [23]:

- obezbeđuje okvir za upravljanje i odlučivanje u oblasti zaštite,
- prilagođava se specifičnim situacijama kroz procedure i uputstva,
- obezbeđuje i integriše principe, standarde i najbolju praksu zaštite,
- obezbeđuje osnovu za evaluaciju usaglašenosti prakse i programa zaštite,
- obezbeđuje dokaz da su mere zaštite implementirane, usaglašene i aktivne, u slučaju spora zbog zloupotreba IKTS ili kompjuterskog kriminala.

Razvoj politike zaštite podrazumeva i razvoj odgovarajućih *procedura*, koje definišu *kako nešto treba uraditi* u oblasti zaštite i opisuju metod kojim se postižu bezbednosni ciljevi, navedeni u politici zaštite, uključujući redosled izvršavanja aktivnosti u procesima zaštite. Kroz procedure se dokumentuju procesi zaštite [35].

3.2.3.1. Struktura i taksonomija politike zaštite

Politika zaštite se može formirati na bazi *zakona*, *standarda* i *iskustva*. Generička struktura *politike zaštite* obuhvata sledeće komponente [5,63,41]:

- *namena i bezbednosni cilj*: svrha i cilj politike zaštite, na bazi zahteva;
- *obim i granice*: oblast i granica na koju se sistema zaštite odnosi;
- *saopštenja:* zahtevi za postizanje *funkcionalnih* ciljeva i *odgovornosti;*
- *zahteve za usaglašenost*: sa zakonom, standardima i praksom zaštite;
- *nametanje i sankcije*: obaveza sprovođenja, disciplinske i druge mere.

U cilju veće korisničke prihvatljivosti i smanjenja kompleksnosti, politika zaštite se može uraditi kao jedinstveni dokument ili na više nivoa: organizacije – *programska politika zaštite*, IKTS – *ISMS politika* i komponenti sistema zaštite – *politika* upotrebe komponente sistema zaštite (npr. *politika udaljenog pristupa*).

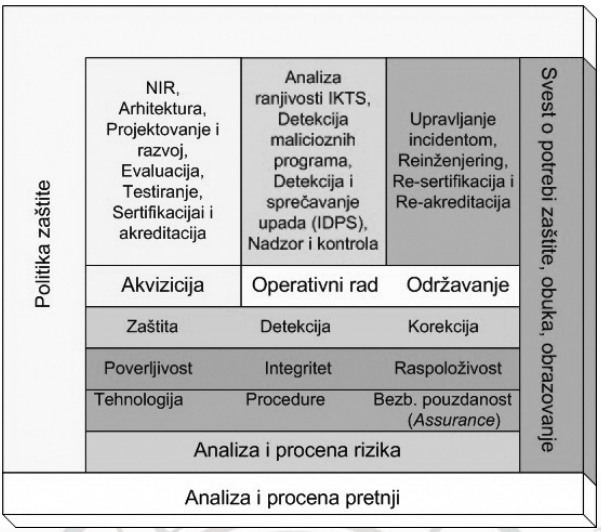
Programska politika obuhvata generičke komponente strukture politike zaštite – *eksplicitnu izjavu o odlučnosti organizacije da zaštiti informacionu imovinu i o odgovornosti i usaglašenosti* i treba da bude koncizna i razumljiva za sve zaposlene, da nameće obavezu izvršavanja i da je relativno nepromenljiva u periodu strateškog plana poslovanja. *ISMS politika* uspostavlja standard za sistem upravljanja zaštitom informacija u organizaciji i navodi specifične bezbednosne ciljeve (npr. obezbediti raspoloživost mrežnih servisa, bezbednost i pouzdanost mrežne infrastrukture, namenu programa zaštite, standarde kriptozaštite itd.). *ISMS politika* eksplicitno navodi za koje komponente sistema zaštite organizacija mora razviti politiku i koji entitet je odgovoran za razvoj i implementaciju. *Politika* upotrebe komponente sistema zaštite obezbeđuje osnovni skup elemenata za definisanje bezbednosnih zahteva za dnevno operativno upravljanje određenom komponentom sistema zaštite, kao što su *udaljeni pristup, upravljanje lozinkom, logička kontrola pristupa, administracija sistema zaštite* itd. Glavni *principi* za razvoj i implementaciju politike zaštite opisani su u Tabeli 3.1 [55]:

Tabela 3.1. Glavni principi za razvoj politike zaštite

Princip	Opis
Obezbediti „bezbednost“ greške	bolje je izgubiti funkcionalnost nego bezbednost
Evidencija bezbednosnih događaja	identifikacija napadača i načina iskorišćenja ranjivosti u logo datoteci bezbednosnih događaja
Jednostavno rešenje mehanizama zaštite	kompleksnost je uzrok brojnih bezbednosnih problema
Jednostavnost upravljanja	lakša provera usaglašenosti i centralno upravljanje
Minimizacija privilegija	davanje prava pristupa, potrebnih za izvršavanje posla
Sprečavanje prelaska sistema u nebezbedno stanje	sistem zaštite vrši svoje funkcije ili blokira pristup
Nemogućnost zaobilaženja mehanizama zaštite	sve tokove informacija u/iz zaštićene RM kontroliše sistem zaštite
Sveopšta podrška zaštiti	kroz teoretsku i praktičnu obuku i praksu zaštite
Razdvajanje dužnosti i odgovornosti	raspodela uloga tako da niko ne može ugroziti kritične procese
Otvoreni dizajn arhitekture sistema zaštite	sistem zaštite ne sme da zavisi od skrivenih implementacija komponenti zaštite
Jačanje zaštite samo slabih komponenti	bezbednost svakog sistema određena je stepenom zaštite najslabije komponente
Potpuna posrednost informacijama	koristiti gde god je moguće kontrolu pristupa, *proxy*, A&A sever itd.
Primena raznovrsnih mehanizama zaštite	primena upravljačkih, operativnih, tehničkih kontrola, da bi napadači morali ovladati različitim veštinama
Korisnička prihvatljivost zaštite	može se obezbediti kroz obuku, povećanje stepena razumevanja i smanjenje kompleksnosti sistema zaštite
Slojevitost mehanizama zaštite	kompromitacija jednog sloja ne ugrožava RS ili RM

Politika zaštite *obezbeđuje* nekoliko funkcija: *okvir za odlučivanje i upravljanje zaštitom, skalabilnost sistema zaštite, integraciju standarda i najbolje prakse i preporuka u program i arhitekturu sistema zaštite, osnova za evaluaciju usaglašenosti prakse i politike zaštite, sistem kontrolnih identifikatora za zaštitu od legalne odgovornosti u slučaju kriminala i dokaz pred sudom da su mere najbolje prakse zaštite bile implementirane, aktivne i usaglašene sa standardima i principima zaštite* (*ISO/IEC 27001, ISO/IEC 13335, CobiT, GAISP, NIST,* ...) [23, 25, 27, 42, 44].

Opšti funkcionalni model za razvoj politike zaštite, koji povezuje sve elemente sistema zaštite, prikazan je na Sl. 3.2. [41, 36].



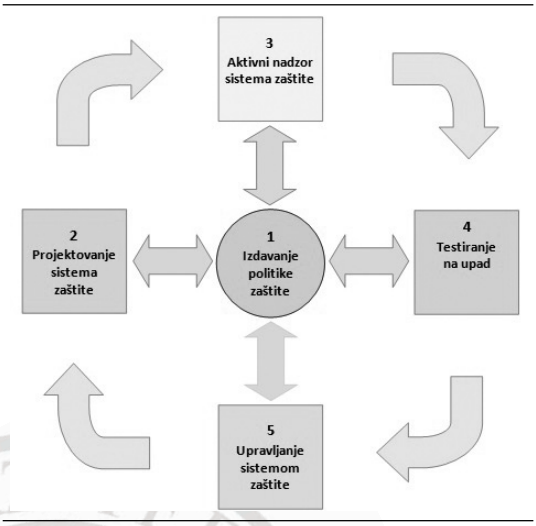
Sl. 3.2. Funkcionalni model za razvoj politike zaštite

Zaposleni moraju politiku zaštite uzeti veoma ozbiljno, a svaki pojedinac prihvatiti odgovornost kao osnov za disciplinske mere, uključujući udaljavanje sa posla i zakonsko gonjenje. *Politika zaštite* treba da ima podršku menadžmenta i da bude:

- razumljiva, racionalna i što je moguće kraća,
- usklađena sa kulturom rada, poslovnim procesima i okruženjem,
- uverljiva korisnicima za postizanje poslovnih ciljeva,
- obavezna i afirmativna (*treba, mora ...* umesto *nikada*, *zabranjeno* i sl.),
- sveobuhvatna i kompatibilna sa politikom organizacije,
- skup *saopštenja* (**šta** treba zaštititi i u **kom** obimu), *informacija* (od kada važi, na koga se odnosi i ko je autor) i *metoda* (za nadzor usaglašenosti),
- instrukcija za obaveznu primenu (ko je odgovoran, sankcije u slučaju neusaglašenosti prakse sa politikom i dopuštena odstupanja),
- skup informacija (kada će se politika preispitivati, koji autoritet vrši reviziju, datum poslednje revizije i da li postoji arhiva politike zaštite),
- baza kontaktnih informacija za izveštavanje o incidentu, sumnjivom ponašanju, anomalijama i indikatorima incidenta i
- uravnoteženi skup efektivnih kontrola zaštite.

U praksi zaštite pogrešno je očekivati da će svi korisnici sprovoditi usvojenu politiku, čak i posle adekvatne obuke. Brzina sa kojom se menjaju faktori rizika, zahteva kontinualan pristup i ažuriranje politike zaštite procesom “ispitaj i popravljaj”. Ovo implicira neprekidan nadzora i kontrolu sistema zaštite i okruženja, ispitivanje ranjivosti, primenu

bezbednosnih popravki, poboljšanje procesa i kontrola zaštite i *ažuriranje politike zaštite* (Sl. 3.3) [41].



Sl. 3.3. Ciklus procesa održavanja politike zaštite

3.2.3.2. Razvoj politike zaštite

Politika zaštite se može odnositi na one aspekte zaštite za koje menadžment smatra da treba da budu tretirani, a u opštoj formi navodi šta je dopušteno, a šta nije u toku rada IKTS i sugeriše šta je od najvećeg značaja i *šta* treba uraditi, a ne *kako* to treba uraditi. Osnovni atributi strukture politike zaštite mogu se definisati na brojne načine, a prihvatljiv skup je: *sadržaj, potreba, namena, pristup u praksi* i *pogodnost za primenu* u specifičnoj situaciji. Ključni kriterijumi za razvoj i generisanje politike zaštite su [10]:

- *funkcija dopunjavanja* internih standarda, uputstava i procedura zaštite;
- *vidljivost za* sve ciljne grupe zaposlenih;
- *menadžerska podrška,* koja garantuje implementaciju politike zaštite;
- *konzistentnost* sa kulturom rada, poslovnim ciljevima i misijom organizacije;
- *eksplicitnost saopštenja,* napisanih opštim, uobičajenim i razumljivim izrazima (*prihvatljivost, neprihvatljivost, neadekvatnost, mora*, *treba* itd.).

U politici zaštite treba nedvosmisleno izraziti *značaj*, što obezbeđuje *smernice*, *osnovu za upravljački okvir*, *uloge i odgovornosti* i *dokumentovati* stav organizacije u odnosu na zaštitu. *Smernice* ukazuju koje aktivnosti treba ili ne treba izvršiti. *Upravljački okviri* na bazi politike zaštite je stabilan u vremenu nepromenljivosti politike. *Uloge i odgovornosti*, za sprovođenje politike u praksi, mora da definiše svaka politika zaštite. *Dokument* politike zaštite eksplicitni izražava stav organizacije prema zaštiti informacija. Ulazne veličine u proces razvoja politike treba da budu rezultati analiza i procena rizika, koji se kasnije mogu koristiti za reviziju adekvatnosti politike u posebnim okolnostima [24, 55].

Saopštenja *(statements)* politike zaštite posebno su efikasan metod za *definisanje specifičnih funkcionalnih zahteva, uloga i odgovornosti* u zaštiti. Koncept ne zavisi od organizacione strukture, a omogućava da se funkcionalni zahtevi i uloge mapiraju sa upravljačkim pozicijama na fleksibilan način. Preklapanja i međuzavisnosti saopštenja

su kritični faktori, koji se moraju korektno kontrolisati, a zahtevi, uloge i odgovornosti koherentno povezivati. Politika zaštite *dokumentuje* i načine rešavanja posebnih pitanja. Iako nema čvrstih i brzo primenjivih pravila za definisanje *forme*, *obima i sadržaja* politike zaštite, brojni uzorci *saopštenja* dostupni su na Internetu (*SANS Institut*, *NIST, Information Shield Policy, ReSecure itd*) [63, 41, 36]. Do konkretnih politika zaštite nije lako doći, jer su poverljivi autorski radovi. Dobar pristup za izradu konkretne politike zaštite obezbeđuje se definisanjem *standardne strukture* zajedničkih i specifičnih elemenata.

Definisanje standardne strukture politike zaštite bitno je za standardizaciju dokumenata zaštite. Jednostavna politika odgovara manjim organizacijama, a za veće su potrebna mnogo preciznija saopštenja i sa više restrikcija. Generalno, *bolje je imati posebnu politiku zaštite na različitim nivoima, nego jedinstvenu*, ali je teško izbeći preklapanja i ponavljanja. Takođe, jedinstvena politika zaštite za veliku organizaciju može biti neprihvatljivo velik dokument.

Politika zaštite može da ima sledeću *opštu strukturu* [35, 41]:

Naslov:
Autor:
Verzija:
Datum:
Amandmani: kontrolni podaci dokumenta, početak primene, datum revizije
Namena: predmet politike i ciljna grupa za koju je dokument namenjen.

---

1. **Uvod**: definicija zaštite informacija, objašnjenje konteksta sistema zaštite.
2. **Struktura, obim i granice**: kratak opis strukture, obima, granica politike.
3. **Bezbednosni ciljevi*:*** svi bezbednosni ciljevi po prioritetima.
4. **Saopštenja**: specifični funkcionalni zahtevi, uloge i odgovornosti, usaglašenost, odnosne politike, sankcije za nespovođenje, vlasnik politike.
5. **Rečnik termina**: ključne reči korišćene u dokumentu.
6. **Odobrava**: poslednja stranica koju potpisuje akreditacioni autoritet

Struktura konkretnog dokumenata politike zaštite na različitim nivoima i za različite komponente zaštite, jednaka je za deo opšte strukture (1 - 3), a razlikuju se za **specifični** deo od tačke 4. - 6. Na primer:

I. Struktura *Programske politike zaštite*:

1– 3. (Tipični deo opšte strukture politike zaštite).

4**.** *Saopštenja politike*

- eksplicitna podrška i kratke smernice za obim i granice politike

4.1. Saopštenje o zahtevima:

- za zaštitu informacija i IKTS organizacije

4.2. Saopštenje o odgovornosti:

- obavezu određivanja uloga (vlasnika) i odgovornosti svih zaposlenih

*4.3. Usaglašenost i obaveza primene***:**

- obavezuje usaglašenosti politike sa standardima i praksom zaštite
- definiše sankcije za nesprovođenje i neusaglašenost politike zaštite

5. *Definicije termina*: rečnik ključnih termina u odnosnoj politici zaštite

6. *Odobrava*:

- potpisuje glavni menadžer

II. Struktura politike zaštite IKTS (*System–Specific Policy*)**:**

1– 3. (Tipični deo opšte strukture politike zaštite)

4**.** *Saopštenja politike*

- eksplicitna podrška i smernice za obim i granice politike;

4.1 Saopštenje o zahtevima:

- za zaštitu specifičnog objekata imovine, komponente, sistema;

4.2 Saopštenje o ulogama i o*dgovornostima:*

- glavnog menadžmenta,
- izvršnih menadžera,
- svih zaposlenih, spoljnih saradnika i TTPS provajdera i
- opštoj odgovornosti za razvoj svesti o potrebi zaštite svih učesnika;

4.3*. Usaglašenost i obaveza primene***:**

- objašnjava hijerarhiju odnosnih dokumenata zaštite i značaj usaglašenosti politike sa standardima i praksom zaštite,
- definiše sankcije za nesprovođenje i neusaglašenost politike zaštite i
- određuje vlasnika politike i listu važnih kontakata (funkcije, ne imena);

5. *Definicije termina*:

- rečnik ključnih termina u odnosnoj politici zaštite;

6. *Odobrava i autorska prava*:

- potpisuje akreditator i obično potvrđuje dobrovoljno ustupanje autorskih prava.

III. Struktura *ISMS politike* zaštite*:*

1. – 3. (Tipični deo opšte strukture politike zaštite)

4. *Saopštenja politike*:

- definicija bezbednosti informacija,
- preporučena lista komponenti zaštite za koje treba razviti politiku, npr: f*izička zaštita, personalna zaštita, upotreba kriptografije, upravljanje kompjuterskim incidentom, logovanje i kontrolni tragovi, udaljeni pristup, zaštita CIA informacija itd.,*

- *uloge i odgovornosti*: detaljne uloge i odgovornosti za ISMS,
- *usaglašenost i obaveza primene i*
- *vlasništvo i kontakti;*

5. Definicije termina

6. Odobrava i autorska prava

ISMS politika (ISO/IEC 27001), između ostalog, treba da sadrži: *definiciju zaštite CIA informacija; bezbednosne ciljeve menadžmenta u oblasti zaštite; uloge i odgovornosti zaposlenih u ISMS; smernice, standarde, procedure i uputstva koji podržavaju politiku ISMS; kratko objašnjenje principa i politike komponenti zaštite; reference o malicioznim programima i napadima; plan kontinuiteta poslovanja; posledice u slučaju kršenja ISMS politike*.

Primer 1: Namena *ISMS politike*: *da zaštiti informacionu imovinu organizacije* **XY** *od svih vidova pretnji. Ovom politikom se definišu funkcionalnost i organizaciona struktura bezbednosti informacija u* **XY***, što se obezbeđuje definisanjem funkcija procesa zaštite kroz saopštenja, uloge i odgovornosti*.

Primer 2: Ciljevi ISMS politike: *da obezbedi zaštitu od neovlašćenog pristupa informacijama; zaštitu poverljivosti, integriteta i raspoloživosti informacija; poslovanje u skladu sa regulativom, zakonima i poslovnim ciljevima; izradu, implementaciju i testiranje planova za kontinuitet poslovanja; dostupnost obuke o zaštiti za sve zaposlene; evidenciju svih sumnjivih događaja u vezi sa bezbednosti informacija i istragu od strane menadžera zaštite informacija*.

Uobičajeno je da *ISMS politika* upućuje na druga dokumenta zaštite, a tipično se menja svake 2 – 3 godine, sa nekom glavnom promenom.

IV. Struktura Politike komponente zaštite (Issue–Specific Policy):

Odnosi se na politiku funkcionalne komponente sistema zaštite. Primer strukture:

1. – 3. (Tipični deo opšte strukture politike zaštite)

4. *Saopštenja:*

- *specifični zahtevi* za, npr. *uskladištene informacije, metod skupljanja informacija, upravljanje kolačićima, pristup ličnim podacima, ažuriranje ličnih podataka, isključivanje informacija*, d*ostupnost za treću stranu* i sl. i
- *uloge i odgovornosti* svih relevantnih učesnika na koje se politika odnosi;

5 i 6. Kao u standardnoj strukturi, ali specifično za konkretnu komponentu zaštite.

Politika komponente zaštite može da se generiše u okviru *Politike zaštite IKTS* kroz specifična saopštenja ili kao samostalni dokument. U prvom slučaju problem je slaba korisnička prihvatljivost obimnog dokumenta, a u drugom – mogućnost ponavljanja i preklapanja.

3.2.3.3. Razvoj procedura zaštite

Procedura je precizno definisan skup, korak po korak, aktivnosti procesa za implementaciju politike zaštite. Sadrži detaljne liste i opšte forme koraka i instrukcija za izvršavanje specificiranih procesa [23, 35]. Značaj procedura zaštite ne sme se nikako potcenjivati, jer su ljudske greške, još uvek, primarni uzrok proboja sistema zaštite. Procedure dokumentuju procese zaštite i opisuju načine implementacije, operativnog korišćenja i odlaganja mehanizama i protokola zaštite. Na primer, procedura za upravljanje kompjuterskim incidentom, treba da *definiše ko i kako upravlja incidentom, kako se skupljaju i istražuju napadi i anomalije u sistemu, kako i kada se interni ili eksterni napad dogodio, ko može objaviti informacije o incidentu i kome ih dostavljati i ko i kako može da izvrši forenzičku istragu, akviziciju i analizu digitalnih dokaza u slučaju kriminala*.

Procedura zaštite spušta politiku na operativni nivo i objašnjava praktične korake „*kako"* se ona implementira u dnevnom radu. Usaglašenost prakse i politike zaštite, u velikoj meri zavisi od toga koliko su kompletne procedure i koliko dobro definišu i opisuju zadatke, koje treba preduzeti, da bi se ispunili bezbednosni ciljevi politike zaštite. Procedure su tipične za *upravljačke* i *organizaciono-operativne* kontrole, koje izvršavaju ljudi i koje se često nazivaju *proceduralne kontrole zaštite.* Za tehničke alate zaštite procedure se uobičajeno daju uz tehničku dokumentaciju [35].

U procesnom pristupu, *procedura zaštite* je sastavna komponenta procesa zaštite, koja opisuje sekvencijalno izvršavanje bazičnih aktivnosti i zadataka, povezuje aktivnosti i određuje redosled izvršavanja zadataka. Procesi zaštite se mogu dekomponovati u tri ključna skupa aktivnosti ili procedura za [35]:

1. upravljanje procesom, koje koordiniraju koherentan rad procesa zaštite,

2. izvršavanje procesa, sa prioritetom izvršavanja i međusobnim vezama i za

3. dokumentovanje kontrola i izlaza procesa zaštite.

Uobičajeno se procesi zaštite normalno dokumentuju kroz *procedure,* koje se, zatim, što detaljnije opisuju u dokumentaciji procesa zaštite. Često treba koristiti zdravu logiku, apriorna i opšta znanja da bi se smanjila kompleksnost, izbeglo nepotrebno ponavljanje i odredio racionalan nivo detalja u svakoj proceduri i dokumentu zaštite. Na taj način pojednostavljuje se proces održavanja sistema zaštite i povećava verovatnoća da će procedure biti stvarno korišćene. Opis procesa zaštite kroz detaljne procedure generiše se u dokumentu *Procedure zaštite* na različitim nivoima (npr. *procedura za administratora zaštite*). Primeri uzoraka procedura zaštite mogu se naći u literaturi [63, 55].

Uputstvo za zaštitu je celovit dokument o zaštiti namenjen *administratorima* i glavnim menadžerima zaštite, kao pomoć u projektovanju sistema zaštite, upravljanju programom zaštite od inicijalnog koncepta do implementacije i u održavanju sistema zaštite, obuci i procesu nadzora, kontrole i revizije. Uputstvo može da sadrži i instrukcije za korišćenje kataloga kontrola zaštite za osnovni i povećani nivo zaštite kritičnih objekata IKTS. Uputstva za zaštitu, *namenjena korisnicima IKTS,* orijentisana su na određene

grupe korisnika i obrađuju određene komponente zaštite u delokrugu odgovornosti te grupe [55].

3.3. PREPORUČENA DOKUMENTACIJA ZA IMPLEMENTACIJU ISMS

Projektna dokumentacija za implementaciju ISMS obuhvata [23]:

- tok procesa implementacije i sertifikacije ISMS;
- definicija obima ISMS;
- ISO/IEC 27002 upitnik/Izveštaj o analizi razlika (*Gap Analysis Report*)
- predlog za implementaciju ISMS;
- plan implementacije ISMS;
- plan tretmana rizika (kako će biti ublažen preveliki rizik);
- saopštenje o primenljivosti – SOA (*Statement of Applicability*);
- inicijative, dnevni red, odobrenja odeljenja za zaštitu informacija;
- strategija upravljanja rizikom, pristup, metodologija;
- organizacija ISMS (dijagram organizacione strukture i izveštavanja);
- rečnik termina zaštite informacija (hiperlinkovani *online* dokument);
- smernice i metrika za implementaciju ISMS (sa idejama i savetima);
- metrika zaštite informacija (skup uzoraka).

ISMS politika, zavisno od konteksta i tipa organizacija, preporučuje izradu:

1. Politika pristupa
2. Politika razvoja svesti o potrebi zaštite i obuka o zaštiti
3. Politika upravljanja rizikom
4. Politika upravljanja životnim ciklusom sistema zaštite
5. Politika prihvatljivog ponašanja
6. Politika zaštite informacija i podataka na komunikacijama
7. Politika upravljanja vanrednim događajem
8. Politika upravljanja kompjuterskim incidentom
9. Politika sakupljanje i održavanje kontrolnih tragova (*Audit trails*)
10. Politika usaglašenosti i odgovornosti
11. Politika sertifikacije i akreditacije
12. Politika čistog stola i ekrana
13. Politika arhiviranja i zadržavanja podataka
14. Politika klasifikacije informacija
15. Politika odlaganje informacija/medija/opreme
16. Politika zaštite e-poslovanja

17. Politika prihvatljive upotrebe e–pošte
18. Politika procene rizika bezbednosti informacija
19. Politika zaštite laptop (mobilnih) računara
20. Politika mobilnog i rada sa daljine
21. Politika upotrebe iznajmljenih resursa (*outsourcing*)
22. Politika upravljanja lozinkom
23. Politika testiranja sistema na proboj
24. Politika personalne zaštite
25. Politika fizičke zaštite
26. Politika zaštite privatnosti
27. Politika upotrebe licencnog softvera
28. Politika antispam zaštite
29. Politika bekapovanja i oporavka sistema/podataka
30. Politika monitoringa upotrebe sistema
31. Politika pristupa treće strane
32. Politika zaštite od malicioznih programa

Osnovni tehnički standardi zaštite (*Baseline Technical Security Standards*) specificiraju bezbednosne konfiguracije i parametre za različite platforme i vrste računara, aplikativne i druge servere, baze podataka, razvojne sisteme, DMZ uređaje, logičke barijere, različite OS, mrežne uređaje, žične i bežične mreže itd.

Procedure za zaštitu informacija tipično uključuju procedure za: *bekapovanje, procenu i reviziju usaglašenosti, izveštavanje o incidentu, reviziju logičke kontrole pristupa, upravljanje bezbednosnim popravkama, administraciju zaštite RS/RM, poboljšanje, testiranje, korisničko održavanje sistema zaštite* itd. Procedure za upravljanje sistemom zaštite tipično uključuju procedure za: *korektivne/ preventivne akcije, registrovanje i dokumentovanje kontrolnih tragova, internu kontrolu i reviziju ISMS, upravljanje rizikom, razvoj svesti o potrebi zaštite, reviziju ISMS, analizu bezbednosnog rizika, programske alate za procenu rizika itd.*

Uloge, odgovornosti i kompetencije *za ISMS* tipično obuhvataju: *lica za planiranje vanrednog događaja i oporavak sistema, vlasnike informacione imovine, analitičare i projektante sistema zaštite, menadžera zaštite informacija – GISO (General Information Security Officer), specijalistu zaštite informacija – ISO (Information Security Officer), specijalistu za testiranje sistema zaštite na proboj, kontrolora sistema zaštite i administratora zaštite RS/RM*.

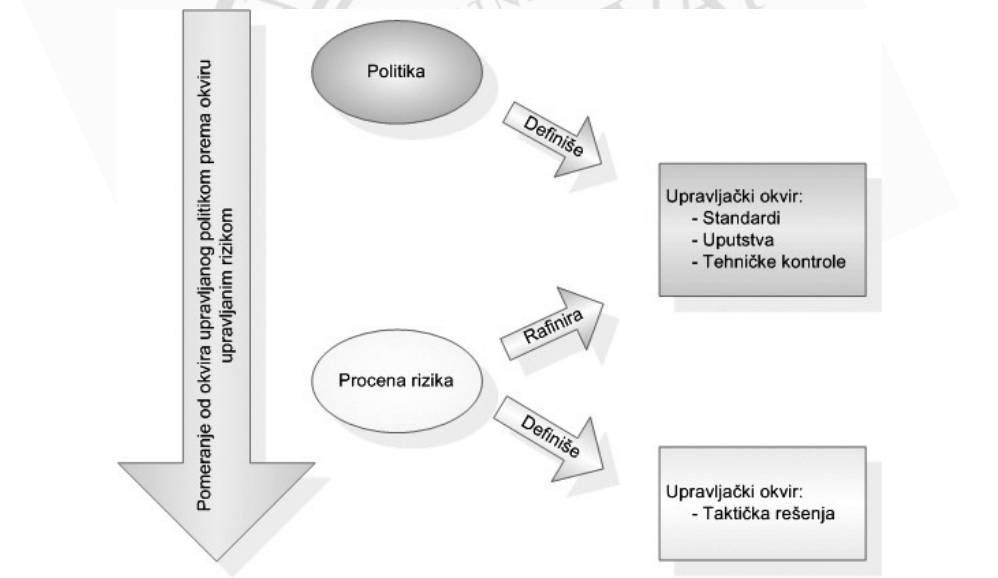
Operativni artefakti su formalne evidencije, koje se generišu kao rezultat ISMS prakse, a čine ih: *plan kontinuiteta poslovanja (BCP); kontrolna lista za procenu uticaja na poslovanje i sistem izveštavanja; plan za oporavak IKTS; templejti za izveštavanje o bezbednosnom incidentu; izveštaji o značajnijim incidentima; lista za proveru i reviziju*

dizajna i arhitekture rešenja za razvoj softvera; taksonomije pretnji i ranjivosti, liste za proveru, upitnici i izveštaji.

Evidencija ISMS obuhvata: *liste baze podataka informacione imovine; registar medija za bekapovanje; registar BCP; registar faktora bezbednosnog rizika; registar kompjuterskih incidenata; lista administratorskih, privilegovanih i korisničkih prava pristupa; registar licenciranih programa; lista standardnih programa RS; registar popravki OS i statusa AVP; registar pristupa TTPS*.

3.4. USPOSTAVLJANJE UPRAVLJAČKOG OKVIRA SISTEMA ZAŠTITE

Upravljački okvir čine saopštenja politike zaštite, standardi zaštite, procedure, radna dokumenta i tehničke kontrole, implementirane da obezbede dnevno operativni rad IKTS. Na slici Sl. 3.5. prikazani su odnosi politike zaštite, procene rizika i upravljačkog okvira sistema zaštite.



Sl. 3.5. Sazrevanje procesa upravljačkog okvira zaštite

Upravljački okvir evoluira sazrevanjem procesa zaštite od upravljanja na bazi politike do implementacije rezultata procene rizika. Upravljanje na bazi politike zaštite, rezultat je strategijskih inicijativa i predstavlja sporo promenljivu komponentu programa zaštite. Upravljanje rizikom je dinamički promenljiva komponenta, a mera u kojoj odgovora

dnevnim potrebama, dobar je pokazatelj zrelosti organizacije. Kako procesi organizacije sazrevaju, očekuje se postepena zamena upravljačkog okvira na bazi politike zaštite, sa upravljanjem na bazi procene rizika, što ukazuje na sposobnost organizacije da brže reaguje na promene u okruženju [55].

Za većinu organizacija upravljački okvir u velikoj meri zavisi od spoljnih partnera i TTPS. Veći je problem za organizacije koje same implementiraju tehnologije zaštite. Na primer, u AVP zaštiti, koja je efikasna u slojevitoj arhitekturi sistema zaštite, incident se može dogoditi, ako se na vreme ne sprovode procedure zaštite. Ovako strog režim zahteva veliku disciplinu, pa rigidna politika zaštite može preživeti uglavnom u vojnoj, policijskoj i državnoj strukturi, a teže u poslovnom okruženju.

Savremeni *koncept upravljačkog okvira sistema zaštite*, uspostavljen na osnovu konsultacija više standarda zaštite (*ISO/IEC 27001 i drugi, PCI–DSS, HIPAA, Gramm–Leach Bliley i NIST*), programa za kontrolu i reviziju i prakse zaštite u više javnih, privatnih i državnih organizacija, obuhvata trinaest *bezbednosnih kategorija komponenti zaštite* na strateškom, taktičkom i operativnom nivo (Tabela 3.2). Cilj je razviti okvir, koji se može integrisati u program zaštite informacija i zadovoljiti strateške potrebe organizacije. Upravljački okvir daje mogućnost organizaciji da modifikuje ili doda kontrole i ciljeve zaštite, da dostigne nivo prihvatljivog rizika, kao i smernice za razvoj, procenu i poboljšanje zaštite informacija.

Tabela 3.2. Bezbednosne kategroije upravljačkog okvira sistema zaštite

Bezbednosne kategorije	Nivo bezbednosne kategorije
(1) organizacija i menadžment	STRATEŠKI
(2) politika zaštite	TAKTIČKI
(3) kontrola, revizija i usaglašenost	
(4) upravljanje rizikom i prikupljanje informacija	
(5) zaštita privatnosti	
(6) upravljanje incidentom	
(7) svest, obuka i obrazovanje u zaštiti	
(8) operativno upravljanje zaštitom	OPERATIVNI
(9) tehničke kontrole zaštite i kontrola pristupa	
(10) monitoring, merenja i izveštavanje	
(11) fizička i zaštita okruženja IKTS	
(12) identifikacija i klasifikacija imovine	
(13) upravljanje nalozima i spoljnim korisnicima	

Nivoi zrelosti i kapaciteti procesa upravljačkog okvira zaštite informacija sa osnovnim karakteristikama dati su u Tabeli 3.3 [22].

Tabela 3.3. Kapaciteti procesa upravljačkog okvira po nivoima zrelosti

Nivo zrelosti	Osnovne karakteristike
Nivo 1	Najbolje prakse se ne izvršavaju, a neformalni procesi nisu planirani.
Nivo 2	Organizacija ima neku politiku i procedure zaštite, najbolje prakse se izvršavaju, procesi su planirani, ali nisu ponovljivi u celoj organizaciji.
Nivo 3	Politika i procedure zaštite su planirane, izvršavane, dobro definisane i implementirane u celoj organizaciji.
Nivo 4	Prakse i procesi zaštite su planirani, izvršavani, dobro definisani, implementirani, kvantitativno upravljani i kontrolisani u celoj organizaciji.
Nivo 5	Prakse i procesi zaštite su planirani, izvršavani, dobro definisani, implementirani, kvantitativno upravljani, kontrolisani u celoj organizaciji, neprekidno poboljšavani i integrisani u strateške poslovne odluke.

3.5. REZIME

Program zaštite uključuje *programsku politiku zaštite, plan zaštite, ISMS politiku*, *politiku komponenti sistema zaštite, procedure* i *uputstva* zaštite. Osnovni zahtevi programa zaštite su sprovođenje nacionalnih i EU zakona i standarda za zaštitu IKTS, kao i obezbeđivanje digitalnih tragova za forenzičku istragu i veštačenje digitalnih dokaza za pravosudne potrebe u slučaju kompjuterskog kriminala. Razvoj svesti o potrebi i obuka u oblasti zaštite, ključne su komponente za implementaciju i održavanje efektivnog programa zaštite. Program zaštite zahteva dokumentovanje svih aktivnosti.

Plan zaštite je sveobuhvatan strategijski set dokumenata projekta za zaštitu informacione imovine. *Politika zaštite* je ključna komponenta plana zaštite, izjava na visokom nivou, koja obezbeđuje okvir očekivanog i obaveznog ponašanja menadžera, zaposlenih, tehnologije i procesa u sistemu zaštite, a realizuje se kroz principe, instrukcije, procedure i smernice, koje su *obavezne* za celu organizaciju. Nametanje obaveze sprovođenja politike zaštite je kritična komponenta programa zaštite, jer ako nema posledica za povrede politike zaštite, zaposleni je neće dosledno sprovoditi. Politika zaštite treba da se prezentira zaposlenima u istom formatu i kroz iste kanale, distribucione liste, uputstva i sl. u organizaciji, kao i poslovna politika organizacije. Politika, standardi, procedure i uputstava zaštite moraju biti realni u pogledu uticaja okruženja, etičkih i kulturoloških principa; moraju biti predstavljeni na takav način da zaposleni shvate da je menadžment odlučan u pogledu njihovog značaja, implementacije i prakse. Standardi, politika, procedure i uputstava zaštite su mehanizmi pomoću kojih menadžment izražava i podržava svoj stav prema zaštiti informacija, kao dragocenoj imovini organizacije. Dok se standardna struktura politike zaštite relativno sporo menja, sadržaj politike, a posebno procedura zaštite, treba da ažurno prati razvoj otvorenih, visoko distribuiranih IKTS i sistema zaštite. Za sistem zaštite potrebna su brojna saopštenja politike zaštite, kao i

procedure zaštite, koji često nisu pod kontrolom centralnog entiteta za upravljanje sistemom zaštite. Politika zaštite treba da obaveže organizaciju na centralizovano upravljanje zaštitom.

Procedure zaštite su precizno definisani načini izvršavanja aktivnosti u primeni politike; propisuju načine implementacije i operativnog korišćenja mehanizama i protokola zaštite i dokumentuju procese zaštite. *Uputstvo za zaštitu* je dokument o zaštiti namenjen administratorima, menadžerima i korisnicima, kao pomoć u radu.

Implementaciju politike i procedura zaštite treba pažljivo planirati u *planu zaštite*, da bi se obezbedila maksimalna efikasnost, sa minimalnim odstupanjem radnih procesa i funkcija. Aktivna podrška menadžera izuzetno je kritična za implementaciju politike.

Upravljački okvir čine saopštenja politike, standardi, procedure, radna dokumenta i tehničke kontrole zaštite. Upravljački okvir na bazi politike je sporo promenljiva komponenta programa zaštite, a na bazi upravljanja rizikom – dinamički promenljiva. Kako procesi organizacije postaju zreliji, očekuje se postepena zamena upravljačkog okvira na bazi politike zaštite, sa procesom upravljanja na bazi procene rizika, što ukazuje na sposobnost organizacije da brže reaguje na promene u okruženju.

3.6. KLJUČNI TERMINI

Plan zaštite: sveobuhvatan dovoljno detaljan, jasan i precizan dokument za planiranje zaštite informacione imovine.

Politika zaštite: izjava na visokom nivou, koja obezbeđuje okvir očekivanog i obaveznog ponašanja menadžera, zaposlenih, tehnologije i procesa zaštite.

Procedure zaštite: precizno definisani načini primene elemenata politike zaštite sa listom detalja i opštih formi koraka specificiranih procesa.

Program zaštite: sve što neka organizacija čini da proizvede, primeni, podrži i unapredi bezbednost IKTS; često se naziva *programska* politika zaštite.

Struktura politike zaštite: standardizovana, metodološka forma izlaganja sadržaja dokumenta politike zaštite, koja obuhvata jedinstven opšti deo za sve tipove politika zaštite i specifični deo za određenu politiku zaštite.

Saopštenje politike zaštite: eksplicitna izjava koju politika zaštite sadrži o određenim pitanjima zaštite; daje se u razumljivoj formi, sa jasnim i jednostavnim terminima.

Upravljački okvir: čine ga politika, standardi i procedure zaštite, radna dokumenta i tehničke kontrole zaštite; sporo promenljiva komponenta programa zaštite.

Upravljačka dokumentacija*:* ugovori, planovi, izveštaji, budžetska dokumenta, NDA i dr.

3.7. PITANJA ZA PONAVLJANJE

1. Dokument Programska politika zaštite treba da obuhvati najmanje:
   a. namenu, bezbednosne ciljeve, obim i usaglašenost
   b. namenu, bezbednosne ciljeve i granice akreditacije
   c. smernice, podršku, odgovornost i odobrenje menadžmenta, komunikaciju, obavezu nametanja politike i sankcije
   d. namenu, bezbednosne ciljeve, usaglašenost (opštu i specifičnu) i odgovornost
2. Generički proces razvoja Plana zaštite obuhvata sledeće osnovne faze:
   a. iniciranje projekta i nabavka resursa za zaštitu
   b. uloge i odgovornosti i upravljanje promenama
   c. razvoj politike zaštite, konsultacije i odobravanje
   d. razvoj svesti, obuka i distribucija politika zaštite
3. Uloga glavne menadžerske strukture u izradi Plana zaštite je:
   a. obezbedi superviziju i definiše i upravlja glavnim smernicama politike zaštite, nadzire i kontroliše realizaciju plana zaštite
   b. pripremi i planira razvoj sistema zaštite i obezbedi projekat implementacije
   c. klasifikuje imovinu, izvrši analizu rizika i preuzme vodeću ulogu i odgovornost u kreiranju programa, plana i politika zaštite
   d. nametne praksu obaveznog uvođenja standarda u oblast zaštite i angažovanja odgovornih, stručnih i iskusnih lica na poslovima zaštite
   e. izvrši internu kontrolu i nadzor sistema zaštite, nametne praksu primene internih standarda i obezbedi usklađenost prakse i programa zaštite
   f. obezbedi eksplicitno izraženu odgovornost menadžmenta, izabere telo za superviziju i kontrolu procesa upravljanja rizikom i sistemom zaštite u celini
4. Opšta procedura za upravljanje promenama treba da ima sledeću osnovnu strukturu:
   a. planiranje, određivanje prioriteta, uvođenje i kataloška registracija promena
   b. uvođenje, kataloška registracija, planiranje redosleda, implementacija i izveštavanje o izvedenim promenama
   c. planski raspored, implementacija i kontrola promena
   d. lista kontrola zaštite za upravljanje promenama i izveštavanje upravne strukture o izvedenim promenama
5. Vrste politika zaštite su:
   a. programska, politika zaštite IKTS, ISMS politika i politika upotrebe komponente sistema zaštite
   b. politika zaštite IKTS, ISMS, politika udaljenog pristupa i politika upotrebe komponente sistema zaštite
   c. programska, politika zaštite IKTS, ISMS politika i politika elektronskog poslovanja
6. Princip za implementaciju politike *Obezbediti bezbednost greške* objašnjava izraz:
   a. preporučuje se primena različitih mehanizama zaštite, da bi maliciozni napadači morali ovladati različitim i po mogućnosti međusobno nespojivim veštinama
   b. ako se greška dogodi, IKTS treba da padne na bezbedan način; *sistem zaštite* treba da ostane u funkciji; bolje izgubiti funkcionalnost nego bezbednost
   c. podrazumeva da svi informacioni tokovi u zaštićenoj mreži i iz nje, moraju prolaziti kroz sistem zaštite informacija i mrežnu barijeru
7. Princip za razvoj i implementaciju politike *Minimizacije privilegija* objašnjava izraz:
   a. samo se u jednostavno i lako upravljanom sistemu može efikasno proveriti usaglašenost konfiguracije komponenti i ostvariti centralno upravljanje.

b. dodeljivanje samo onih korisničkih i adminstrativnih prava pristupa koja su neophodna za izvršavanje dužnosti
c. pod očekivanim okolnostima sistem zaštite ili potpuno izvršava svoje funkcije ili potpuno blokira pristup.
d. preporučuje se primena različitih mehanizama zaštite, da bi maliciozni napadači morali ovladati različitim i nespojivim veštinama za proboj sistema zaštite

8. Princip za razvoj i implementaciju politike zaštite *Odvajanje dužnosti* objašnjava izraz:
   a. mehanizmi zaštite i IKTS generalno treba da bude što je moguće jednostavniji, jer je kompleksnost uzrok brojnih bezbednosnih problema
   b. raspodela uloga i odgovornosti u sistemu zaštite i IKTS u kojoj jedan čovek ne može narušiti kritične procese organizacije
   c. garantovana bezbednost svakog sistema zaštite određena je stepenom zaštićenosti najslabije komponente, što često nije ni računar, nego čovek
9. Princip za razvoj i implementaciju politike zaštite *Jačanje zaštite samo slabih komponenti* objašnjava sledeći izraz:
   a. garantovana bezbednost svakog sistema zaštite određena je stepenom zaštićenosti najslabije komponente, što često nije ni računar, nego čovek
   b. funkcije u zaštiti do najvećeg mogućeg stepena treba da budu odvojene; koncept treba primeniti i na sisteme i operatere/korisnike.
   c. treba koristiti svuda indirektan pristup informacijama, preko *posrednih elemenata* koji nameću politiku zaštite (AC, *proxy i A&A* server, e-mail *gateway*)
10. Princip za razvoj i implementaciju politike zaštite *Slojevita zaštita* objašnjava izraz:
    a. korisnici treba da razumeju potrebu zaštite, što se može obezbediti kroz obuku, a implementirani mehanizmi treba da pruže osećaj korisnosti
    b. pojedinačni mehanizam zaštite generalno je nedovoljan, mehanizmi zaštite treba da budu slojevito raspoređeni u arhitekturi sistema zaštite, tako da kompromitacija jednog ne ugrožava host sistem/mrežu
    c. kada su sistem i mreža kompromitovani, to treba registrovati ili evidentirati u *log* datoteci, a ove *kontrolne informacije* mogu pomoći kod identifikacije načina iskorišćenja ranjivosti, identifikacije napadača i proboja slojevite zaštite
11. Ključne funkcije politika zaštite su:
    a. opisuje *šta treba raditi* u oblasti zaštite i obezbeđuje okvir očekivanog i obaveznog ponašanja menadžera, zaposlenih, tehnologije i procesa
    b. obezbeđuje potrebnu dokumentaciju zaštite i skup kontrola za osnovnu zaštitu
    c. utvrđuje ciljeve, očekivanja i verifikovane korisničke zahteve za poslovne procese
    d. koristi principe, instrukcije, procedure i smernice, obavezne za organizaciju
12. Ključni kriterijumi za razvoj i generisanje *politike zaštite su*:
    a. jasno razumevanje vizije i ciljeva zaštite od strane menadžera, uključivanje specijalista zaštite, informatičara i što više predstavnika organizacionih jedinica
    b funkcija dopunjavanja, vidljivost, menadžerska podrška, konzistentnost i eksplicitnost saopštenja
    c. identifikovani glavni rizici za informacionu imovinu i razvijen projekat sistema zaštite, koji reflektuje potrebe organizacije
13. Navedite obavezne sastavne komponente tipične strukture politike zaštite:
    a. namena, cilj, vrsta, obim, odgovornost, usaglašenost, saopštenja
    b. namena, cilj, vrsta, obim, odgovornost, usaglašenost

c. namena, cilj, obim, specifična saopštenja, odgovornost, usaglašenost, sankcije
d. namena, obim, specifična saopštenja, odgovornost, usaglašenost, sankcije

14. Navedite saopštenja/zahteve koja se mogu naći u *Politici lozinke*:
    a. ne menjati lozinku najmanje tri meseca
    b. menjati lozinku najmanje jedanput mesečno
    c. uzimati što kraću i jednostavniju lozinku zbog lakšeg pamćenja
    d. zapisivati lozinku da bude na dohvat ruke, da se lakše koristi
    e. čuvati lozinku na bezbednom mestu
    f. koristiti lozinku sa najmanje 8 karaktera kombinovanih interpunkcijskih znakova slova i brojeva
15. Koja vrsta politike uobičajeno zabranjuje igranje računarskih igrica na poslu:
    a. politika kontrole pristupa
    b. politika udaljenog pristupa
    c. politika ispravnog ponašanja u IKTS
    d. politika minimuma privilegija
16. Procedura zaštite je:
    a. precizno definisan skup, korak po korak, aktivnosti procesa zaštite
    b. komponenta procesa zaštite koja opisuje aktivnosti i određuje tok procesa
    c. skup povezanih aktivnosti zaštite, koje čini proces upravljanja zaštitom
    d. način implementacije i operativnog korišćenja mehanizama i protokola zaštite
17. ISMS standard (ISO/IEC 27001) obezbeđuje:
    a. uputstvo za upravljanje i izbor kontrola zaštite
    b. odgovore kako treba upravljati zaštitom
    c. instrukcije šta treba raditi u praksi zaštite
    d. upravljačke, operativne i tehničke kontrola zaštite
    e. tehnički standard za specifične tehnologije i metriku za evaluaciju zaštite
    f. sistem za upravljanje zaštitom informacija
    g. kompatibilnost sa SSE CMM modelom sazrevanja procesa zaštite
18. Kontrolni okvir je:
    a. skup politika, standarda, procedura, radnih dokumenata i kontrola zaštite
    b. rezultat strategijskih inicijativa i dugoročnih bezbednosnih ciljeva
    c. rezultat kratkoročnih taktičkih bezbednosnih zahteva
    d. sporo promenljiva komponenta programa zaštite
    e. pokazatelj zrelosti procesa zaštite organizacije
    f. upravljan politikom zaštite i procesom procene rizika
    g. uvek zavisi od spoljnih partnera (poverljivih provajdera servisa zaštite – TTPS).

4. NADZOR, KONTROLA I REVIZIJA SISTEMA ZAŠTITE

Po završetku ovog poglavlja razumećete:

- principe i značaj servisa za nadzor, kontrolu i reviziju zaštite
- razvoj procesa za nadzor, kontrolu i reviziju sistema zaštite
- strategije za nadzor, kontrolu i reviziju sistema zaštite
- značaj razvoja kapaciteta (tim, alati) za nadzor, kontrolu i reviziju
- značaj analize rezultata nadzora, kontrole i revizije sistema zaštite

4.1. UVOD

Savremeni poslovni IKTS sve više zavise od sistema zaštite. Da bi se izbegli ili sprečili brojni rizici, nužno je obezbediti neprekidan nadzor, kontrolu i reviziju[32] (*auditing)* sistema zaštite. Kontrolori i revizori zaštite moraju biti osposobljeni za evaluaciju sistema zaštite i da ponude preporuke za smanjenje bezbednosnog rizika na prihvatljivi nivo.

Praksa *nadzora, kontrole i revizije sistema* zaštite ukazuje na brojne ranjivosti IKTS, kao što su: *nedostatak formalnog plana i politike zaštite; neadekvatnost kontrola zaštite; nepotpuno korišćenje NOSSS kapaciteta zaštite; instalacija/modifikacija programa bez kontrole i izmene pretpostavljene konfiguracije ili lozinke; neažuriranje definicija AVP; neadekvatnost planova za vanredne događaje i kontinuitet poslovanja; neadekvatnost odgovornosti u zaštiti; sporo objavljivanje otkrivenih ranjivosti; nedovoljna svest o potrebi zaštite; velika ovlašćenja i slabo razdvajanje dužnosti u IKTS; nedostatak osnovnih kontrola za upravljanja programom zaštite itd.* Posebnu pažnju kontrolori i revizori sistema zaštite treba da usmere na implementaciju kontrola zaštite i upravljanje zaštitom.

4.2. PROCESI NADZORA, KONTROLE I REVIZIJE SISTEMA ZAŠTITE

Interni nadzor i kontrola sistema zaštite treba da budu stalne, povremene i regularne aktivnosti, koje se vrše u skladu sa definisanom procedurom. *Kontrolni tragovi* su zapisi bezbednosno relevantnih događaja u *bezbednosnoj log* datoteci, a koriste se za otkrivanje proboja, neovlašćenog korišćenja i eventualne zloupotrebe informacija i objekata u RS/RM. Zavisno od konfiguracije, mogu biti ograničeni na specifične bezbednosne događaje ili da obuhvataju sve aktivnosti u sistemu.

32 Termin *revizija* podrazumeva *tehničku reviziju* sistema zaštite, za razliku od *finansijske revizije.*

Funkcija revizije sistema zaštite obezbeđuje internu i nezavisnu (eksternu) evaluaciju politike, procedura, standarda, kontrola i prakse zaštite IKTS od gubitaka informacija, oštećenja, nenamernog otkrivanja ili pada sistema. Mehanizmi za reviziju sistema zaštite treba da obezbeđuju reviziju svakog pristupa sistemu i osetljivim informacijama [38].

Bezbednosni ciljevi nadzora, kontrole i revizije zaštite su obezbeđenje dodatnog faktora poverenja korisnika u zaštitu i provera ispravnosti rada i korišćenja različitih mehanizama višeslojne zaštite, obrazaca pristupa objektima IKTS, istorije pristupa specifičnih procesa i korisnika, ponovljenih pokušaja ovlašćenih i neovlašćenih korisnika da zaobiđu mehanizme zaštite, korišćenja privilegija i dr.

Korisnici mehanizma za nadzor, kontrolu i reviziju mogu se podeliti u grupe *kontrolora*, *revizora* i *korisnika*. *Kontrolori i revizori* su korisnici sa sertifikovanim pravima – administratori sistema (za niže nivoe kontrole i revizije) ili administratori zaštite, koji biraju događaje, koje sistem treba da registruje, postavljaju kontrolne markere za registrovanje događaja i analiziraju kontrolne tragove. *Korisnici* su administratori, operateri, programeri i drugi korisnici IKTS, koji generišu kontrolne događaje i moraju razumeti da postoje mehanizmi za nadzor, kontrolu i reviziju i koji uticaj oni imaju na njih, što je presudno za faktore odvraćanja i postizanja bezbednosnih ciljeva.

4.2.1. Glavni aspekti procesa kontrole i revizije sistema zaštite

Standarde i uputstva za nadzor, kontrolu i reviziju zaštite IKTS donosi nekoliko međunarodnih organizacija, od kojih su najznačajnije **ISACA** (*The Information Systems Audit and Control Association*) i **ISACF** (*The Information Systems Audit and Control Foundation*), koja je izdala set uputstava za kontrolu sistema zaštite – **COBIT** (*Control Objectives for Information and Related Technology)* [19, 27].

Entiteti za nadzor, kontrolu i reviziju treba da razviju kapacitete, adekvatne veličini, strukturi i potrebama organizacije. Obavezu nadzora, kontrole i revizije sistema zaštite, treba obuhvatiti u normativno regulisati nacionalnim *Zakonom o zaštiti informacija*. Na bazi normativnog okvira i usvojenih standarda, svaka organizacija može izraditi *Uputstvo za nadzor, kontrolu i reviziju sistema zaštite*, koje treba da uključi *planiranje, razvoj, implementaciju, merenje funkcionalnosti i poboljšanje kapaciteta za nadzor, kontrolu i reviziju sistema zaštite IKTS* [38].

Glavni mehanizmi za nadzor, kontrolu i reviziju sistema zaštite IKTS su:

Identifikacija i autentifikacija, koja obezbeđuje logovanje na sistem i normalno zahteva da korisnik unese korisničko ime i neki identifikator za autentifikaciju. Bez obzira da li su ove informacije validne ili ne, izvršavanje procedure logovanja je kontrolni događaj, a unesena informacija u log datoteku smatra se kontrolnom informacijom. U slučaju da unesena informacija nije prepoznata kao validna, sistem ne treba da je evidentira u log datoteku. Razlog za to je, što korisnik može greškom uneti lozinku, kada sistem traži korisničko ime za logovanje. Ako se informacija upiše u kontrolni trag,

kompromitovaće lozinku i bezbednost sistema. Savremeni OS sprečavaju upisivanje lozinke u log datoteku kontrolnih tragova, pa je ovaj rizik izbegnut. Prednost registrovanja identifikacionih parametara (*credentials*) je, što olakšava otkrivanje pokušaja proboja sistema zaštite i identiteta napadača u fazi digitalne forenzičke istrage kompjuterskog incidenta.

Administracija uključuje odgovorna lica, koja operativno upravljaju kapacitetima i sprovode procedure za nadzor, kontrolu i reviziju sistema zaštite [38].

Projekat rešenja treba da sadrži mehanizam, koji poziva funkciju evidencije kontrolnih tragova, na zahtev administratora zaštite i koji određuje da li događaj treba da bude unesen u log datoteku kao kontrolni trag. Kontrolori i revizori moraju izabrati bezbednosno relevantne događaje za registrovanje u log datoteku kontrolnih tragova i rekonfigurisati log datoteku, na bazi identiteta korisnika, bezbednosne klasifikacije objekata IKTS ili procene rizika.

Zaštita kontrolnih mehanizama i osetljivih podataka kontrolnih tragova u log datoteci, od neovlašćenog pristupa je obavezna. Uklonjeni mediji, koji sadrže kontrolne tragove, moraju se fizički zaštititi i odlagati u skladu sa propisanom procedurom fizičke zaštite i saniranja osetljivih elektronskih medija za ponovnu upotrebu. Glavni bezbednosni zahtevi za kontrolni mehanizam i kontrolne tragove su *zaštita od neovlašćenog pristupa, modifikacije ili zaobilaženja i aktiviranje/ dezaktiviranje kontrolnih mehanizma i zaštita kontrolnih tragova sa NOSSS mehanizmima zaštite, nepristupačnim za neovlašćene korisnike* [55].

4.2.2. Planiranje nadzora, kontrole i revizije sistema zaštite

Plan ili poboljšanje procesa nadzora, kontrole i revizije sistema zaštite treba da sadrži sledeće korake:

a. definisanje misije, ciljeva, obima i granica razvoja kapaciteta,
b. procena tekućih kapaciteta za nadzor, kontrolu i reviziju sistema zaštite,
c. planiranje procesa nadzora, kontrole i revizije i
d. planiranje sistema za merenje i monitoring rezultata kontrole i revizije.

a. Definisanje misije, ciljeva, obima i granica za razvoj kapaciteta za nadzor, kontrolu i reviziju sistema zaštite, treba planirati najmanje za tri godine sa eksplicitnim navođenjem odgovornosti menadžera i izvršioca, identifikovanjem tipova alata, potrebnih znanja, veština i obuke kontrolora i revizora. Najznačajniji ciljevi su: *obezbediti podršku za poboljšanje procesa, dopuniti proces sa procenom efektivnosti sistema zaštite, obezbediti nezavisnu reviziju zaštite za procenu rizika, podržati zahteve za korporacijsku digitalnu forenzičku istragu, obezbediti podršku za analizu i ekstrakciju podataka i obezbediti mišljenje revizora zaštite u procesu razvoja sistema zaštite.* U izgradnji kapaciteta za nadzor, kontrolu i reviziju zaštite treba: *proceniti kapacitete i*

rentabilnost implementacije sa datim resursima, konsultovati zakon za kompjuterski kriminal, definisati potencijalne odgovornosti, izvršiti bezbednosnu proveru (posebno TTPS) i razmotriti zakon za obavezan pristup informacijama [35].

Definisanje obima i granica nadzora, kontrole i revizije zaštite uključuje relevantne učesnike i kapacitete za izvršavanje zadataka. Kontrolor i revizor prikupljaju informacije o infrastrukturi IKTS na osnovu upitnika [63]. U praksi zaštite, organizacije vlastitim kapacitetima, uglavnom, planiraju samo proces nadzora, interne kontrole i revizije, dok regularnu godišnju reviziju (*audit*) vrše spoljni, nezavisni i akreditovani revizori ili revizorski timovi.

b. Procena postojećih kapaciteta za nadzor, kontrolu i reviziju sistema zaštite uključuje identifikaciju objekata IKTS i bezbednosnog rizika procesa revizije, kao prvi korak**.** Teško je očekivati da jedan revizor ima sva potrebna znanja i sposobnosti, pa se preporučuje formiranje tima. Sakupljanje i dokumentovanje informacija o sistemu, podacima i aplikacijama može da obuhvati brojna pitanja, kao što su: *značaj i prirodu programa i servisa sistema zaštite, osetljivost (CIA) procesiranih informacija, tipove računara za procesiranje, specifične platforme, uslužne programe, alate za restrikciju pristupa programima i podacima, nivo umrežavanja, barijere i druge mrežne uređaje, tipove i obim važnijih komercijalnih i programa razvijenih u organizaciji, način i mesto unosa podataka i izveštavanja, približan broj transakcija i vrednosti koje procesira svaki sistem, organizacione promene i ključni personal zaposlen u IKTS, oslanjanje na druge organizacije u procesiranju, rezultate poslednje revizije i usaglašenost.*

Formiranje tima za reviziju, procena znanja, sposobnosti i veština internih i iznajmljenih članova, ključne su komponente planiranja, izgradnje ili unapređenja kapaciteta za reviziju zaštite. Z*nanja* i *veštine* revizora zaštite, rangiraju se kao:

- *stručnjak (ekspert)* – ima veliko iskustvo, može instruisati druge revizore,
- *profesionalac* – može izvršiti zadatke revizije bez posebnih priprema,
- *sposoban* – veruje da može izvršiti zadatke, ali zahteva pomoć i
- *motivisan* – ima jaku želju i interes za sticanje znanja i veština za reviziju.

Profil *stručnjaka* najčešće se određuje parametrom *znanja, veština i sposobnosti* – **KSA** (***K****nowledge,* ***S****kills,* ***A****bilities*), koji se tipično koristi za opisivanje radnih mesta i oglašavanje za slobodna radna mesta, ukazujući na zahtevane atribute [18].

Znanje je organizovan i usvojen korpus informacija, činjenica, principa/procedura, čija primena omogućava izvršavanje posla i predstavlja osnovu za izgrađuju veština i sposobnosti. *Veština* je sposobnost manuelnog, verbalnog ili mentalnog manipulisanja ljudima, idejama i stvarima, koja se može demonstrirati. *Sposobnost* je mogućnost za izvršavanje nekih poslovnih funkcija, koristeći bitna znanja, a dokazuje se kroz aktivnosti, koje se zahtevaju za obavljanje nekog posla [18]**.**

I dentifikacija i izbor automatizovanih alata za reviziju zaštite, kao i sertifikovanih revizora, koji poseduju znanje i veštinu za njihovu upotrebu, kritični su faktori za identifikovanje ranjivosti sistema.

Primer: *alati za ekstrakciju podataka* u programu za logičku kontrolu pristupa, mogu identifikovati kršenje principa razdvajanja dužnosti privilegovanih korisnika; *krekeri lozinki* mogu identifikovati pretpostavljene/slabe lozinke; *sniferi* mogu identifikovati otvoren prenos lozinki ili osetljivih informacija; s*keneri* identifikuju zaštitni profil RS/RM itd.

Većina organizacija koristi usluge specijalizovanih revizora/revizorskih organizacija u procesu izbora adekvatnih *automatizovanih alata za reviziju sistema zaštite*, kao i u procesu obuke i izbora revizora za njihovo korišćenje. Bilo da formira ili modernizuje kapacitete za reviziju sistema zaštite, organizacija treba da razvije proces selekcije, evaluacije i revizije programskih alata za reviziju zaštite, kroz: *istraživanje raspoloživih alata i izbor iz svake kategorije, razmenu iskustava sa partnerima o pogodnosti alata, određivanje procesa za kontrolu rentabiliteta alata, potrebe za alatima za specifične platforme, metodologije za evaluaciju, izbor i razvoj procedure za obuku korisnika.*

Razvoj metodologije za izbor i implementaciju programskih alata za reviziju sistema zaštite ima višestruke prednosti: *izabrani alat je koristan za tim i proces revizije, ne gubi se vreme na neadekvatne alate, minimiziraju se organizacioni uticaj i troškovi obuke, obezbeđuju se efektivnije preporuke revizora i obuka i stiču neophodna znanja revizora/tima.* Izbor alata je kritičan faktor za razvoj kapaciteta za reviziju zaštite.

Procena troškova procesa revizije nezaobilazno je pitanje, pošto obuka, iznajmljivanje konsultanata i održavanje kapaciteta za reviziju zaštite zahtevaju značajne troškove.

c. **Planiranje procesa revizije sistema zaštite** može uključiti sopstvene ili iznajmljene kapacitete. Organizacija koja ima razvijene kapacitete za reviziju sistema zaštite, treba da definiše kriterijume za planiranje i izbor projekata za reviziju, koji mogu uključivati *kritičnost i procenu rizika sistema za reviziju, saradnju vlasnika sistema za redukciju rizika u toku testiranja, nivo kompleksnosti sistema za reviziju, godišnji i kratkoročni plan revizije* itd. Generalno, kod planiranja revizije, treba koristiti *rotacioni* metod za izbor sistema za regularnu godišnju reviziju. Metod je posebno značajan za planiranje revizije zaštite u visoko distribuiranim sistemima.

   Za izgradnju ili dogradnju kapaciteta za reviziju sistema zaštite, zahteva se veliki broj aktivnosti, koje variraju u zavisnosti od ciljeva revizije. Mogu se razviti *radni dokumenti,* koji pomažu da se *uspostave i povežu ciljevi i aktivnosti i identifikuju potrebni resursi*. Resursi za planiranje, razvoj i održavanje kapaciteta za reviziju mogu se naći na brojnim *web* lokacijama (*www.isaca.org, www.itaudit.org, www.auditnet.org,www.cert.org, www.sans.org*).

d. **Planiranje procesa merenja i monitoringa rezultata revizije** obavezno je za revizorske organizacije, radi procene i poboljšanja performansi sistema za reviziju. Treba jasno definisati misiju i ciljeve revizije i uspostaviti dugoročni/kratkoročni plan rada. Rezultate merenja performansi sistema za reviziju treba porediti sa uspostavljenim ciljevima i izveštavati o progresu.

Primeri ciljeva revizije zaštite: *regularna revizija, evaluacija rezultata i preporuke; evaluacija usaglašenosti rezultata revizije i standarda/zakona; atraktivnost kapaciteta za reviziju za visoko kvalifikovane, motivisane i posvećene stručnjake; poverenje, otvorenost komunikacije i profesionalni rezultati u radnom okruženju* itd. [35].

U procesu revizije treba definisati sistem indikatora performansi (*benčmarking sistem*) internih i eksternih kapaciteta za reviziju.

Primer: *benčmarking kompetentnosti tima za reviziju*, zahteva da svako IKT odeljenje ima 65% revizora sa sertifikatom CISA (*Certified Information Systems Auditor*) ili diplomom informatičara ili menadžera IKTS.

Evaluaciju procesa revizije treba vršiti periodično da bi se procenio stvarni progres u postizanju dugoročnih ciljeva revizije. *Procenu korisničke prihvatljivosti* procesa i servisa revizije, treba vršiti u regularnim intervalima, da bi se identifikovale slabosti i postavili ciljevi za poboljšanje kapaciteta za reviziju. U entitetu gde se vrši revizija treba izvršiti anketu za procenu *profesionalizma tima za reviziju, tehničkog razumevanja oblasti revizije, komunikacionih sposobnosti revizora, efektivnosti korišćenja raspoloživih resursa, sposobnosti održavanja pozitivnih i produktivnih odnosa i profesionalizma u izveštavanju o nalazima revizije*. *Izveštaje o progresu* procesa revizije, dostavljati menadžmentu kontrolisane organizacije i, zavisno od nalaza, inicirati odgovarajuće akcije. Primeri ciljeva i metrike revizije sistema zaštite prikazani su u Tabeli 4.1.

Tabela 4.1. Ciljevi i metrike kontrole i revizije sistema zaštite

Cilj revizije sistema zaštite	Metrika
Vreme revizije ne premašuje budžet više od 10%	Akumulirati sva realna vremena, uporediti sa finansiranim vremenom revizije i odrediti kumulativni premašaj/ podbačaj za sve izvršene procese revizije
90% procesa revizije završiti u datom roku (npr. 6 meseci)	Odrediti % procesa revizije završenih u specificiranom roku (na bazi izveštaja)
80 % izveštaja izraditi 30 dana od završetka revizije	Odrediti % izveštaja dostavljenih u planiranom roku (od završetka revizije do dostavljanja izveštaja)
90 % preporuka iz izveštaja treba da prihvati menadžment	Odredi % preporuka iz izveštaja prihvaćenih u formalnom odgovoru menadžmenta
Implementirati 60 % preporuka iz izveštaja u nekom periodu	Odredi procenat preporuka iz izveštaja, implementiranih u određenom periodu

Glavni kriterijumi za ocenu rezultata revizije, za definisane strateške ciljeve su *poboljšanje sistema, procesa i metodologije zaštite*. *Izveštaj o rezultatima revizije,* koji revizor dostavlja u planiranom roku menadžmentu kontrolisane organizacije, treba da sadrži: *ciljeve, period rada, prirodu i obim izvršenih aktivnosti, primenjene standarde, organizaciju i lica kojima se dostavlja, eventualne restrikcije o cirkulisanju, nalaze, zaključke i preporuke, sve rezerve ili kvalifikacije koje revizor ima u odnosu na proces revizije i iskaz da li su u procesu revizije i izveštavanja otkrivene informacije, koje mogu kompromitovati kontrolisani sistem*. Za *merenje aktivnosti posle procesa revizije* zahteva se uspostavljanje procedure za preduzimanje akcija.

4.3. REZIME

Glavni principi, koji obezbeđuju uspostavljanje efikasnih i efektivnih kapaciteta (revizora/tima, tehnika i alata, resursa za podršku) za kontrolu/reviziju zaštite IKTS, obuhvataju: *planiranje i definisanje funkcija i ciljeva, mehanizama, korisnika mehanizama i drugih aspekata procesa za kontrolu/reviziju zaštite*.

Na bazi normativa i standarda treba definisati, vlastite ili iznajmljene, kapacitete za reviziju zaštite – planirati proces revizije i izraditi *Uputstvo za nadzor, kontrolu i reviziju zaštite IKTS*, koje mora obuhvatiti, najmanje, procese planiranja, razvoja kapaciteta, implementacije mehanizama i nadzora funkcionisanja i evaluacije kvaliteta procesa i rezultata kontrole/revizije. Za izradu plana, modifikaciju ili poboljšavanje procesa kontrole/revizije, treba definisati misiju i ciljeve razvoja kapaciteta, proceniti postojeće kapacitete, planirati dinamiku procesa, povezati ciljeve sa aktivnostima procesa i obezbediti istraživanje i obuku za kontrolu/reviziju.

Ključna komponenta kapaciteta je tim za kontrolu/reviziju, uključujući procenu znanja, sposobnosti i veština – **KSA** kontrolora/revizora prema skali: *profesionalac, stručnjak, osposobljen i jako zainteresovan.* Za poslove kontrole/revizije potrebni su veliko iskustvo i specifične veštine.

Razvoj metodologije za izbor i implementaciju softverskih alata za reviziju sistema zaštite ima višestruke prednosti za formiranje ili modernizuju kapaciteta za reviziju. Revizorske organizacije, treba da monitorišu funkcionisanje procesa revizije, mere performanse i rezultate svakog procesa i izaberu indikatore progresa procesa revizije. Revizor/tim dostavlja izveštaj o reviziji, poverljivim kanalima, uz garanciju da proces revizije nije kompromitovao kontrolisani IKTS, a rezultati i komentari ostaju u vlasništvu kontrolisanog entiteta. Posle dostavljanja izveštaja treba uspostaviti proceduru, koja obavezuje menadžment kontrolisanog entiteta da preduzme odgovarajuće akcije u predviđenom roku, a na bazi nalaza i preporuka revizora.

4.4. KLJUČNI TERMINI

Bezbednosno–relevantni događaj (*Security–Relevant Event***):** događaj koji pokušava da izmeni bezbednosno stanje sistema ili naruši politiku zaštite sistema.

Kontrolni događaj (*Auditable Event***)**: događaj koji se može izabrati i logovati u datoteku kontrolnih tragova, kao bezbednosno relevantan za oporavak sistema.

Mehanizam za reviziju (*Audit Mechanism***):** hardversko softverski modul koji se koristi za skupljanje, pregled i/ili ispitivanje aktivnosti sistema.

Kontrola sistema zaštite (*Security System Control***):** povremena analiza rezultata nadzora sistema zaštite.

Kontrolni trag (*Audit Trail*)**:** skup registrovanih podataka koji obezbeđuju dokumentovane dokaze o procesima za praćenje traga od originalne transakcije do odnosne snimljene informacije i izveštaja, ili unazad od snimljene informacije i izveštaja do izvora transakcije.

Nadzor sistema zaštite (*Security System Monitoring***):** neprekidna aktivnost opservacije funkcionisanja mehanizama i servisa zaštite.

Revizor (*Auditor*): ovlašćeno lice sa pravima izbora događaja za reviziju, podešavanja sistema za registrovanje tih događaja i analize kontrolnih tragova.

Revizija (*Audit***)**: proces interne ili eksterne (nezavisne) tehničke revizije i ispitivanja servisa, mehanizama, prakse, procesa upravljanja i dokumentacije sistema zaštite.

4.5. PITANJA ZA PONAVLJANJE

1. Ključni bezbednosni ciljevi nadzora, kontrole i revizije sistema zaštite su da:
   a. proveri ispravnost rada i korišćenja različitih mehanizama višeslojne zaštite
   b. omogući podizanje svesti o potrebi zaštite i odvraćanje napadača
   c. obezbedi dodatni faktor poverenja korisnika u sistem zaštite
   d. obezbedi kontrolu i reviziju obrazaca i istorije pristupa objektima IKTS specifičnih procesa i korisnika
   e. obezbedi kontrolu i reviziju obrazaca ponovljenih pokušaja ovlašćenih i neovlašćenih korisnika da zaobiđu mehanizme zaštite i korišćenja privilegija
2. Glavni bezbednosni zahtevi za mehanizam za kontrolu i reviziju sistema zaštite:
   a. mehanizam za registrovanje kontrolnih tragova mora biti zaštićen od neovlašćenog pristupa, modifikacije ili zaobilaženja
   b. kontrolni trag zaštićen sa NOSSS mehanizmom od neovlašćenog pristupa i izmene
   c. aktiviranje/dezaktiviranje mehanizma za reviziju treba da bude deo NOSSS mehanizama zaštite i nepristupačan za neovlašćene korisnike
   d. kontrolni trag transparentan i na raspolaganju svim korisnicima IKTS
3. Za izradu plana ili poboljšavanje procesa nadzora, kontrole i revizije zaštite treba:
   a. definisati misiju, ciljeve, obim i granice razvoja kapaciteta za kontrolu/reviziju
   b. definisati preostali, prihvatljivi rizik
   c. proceniti vlastite kapacitete za kontrolu/reviziju sistema zaštite
   d. planirati proces kontrole/revizije sopstvenim ili iznajmljenim kapacitetima
   e. planirati proces za sertifikaciju sistema zaštite i

f. planirati sistem merenja procesa kontrole/revizije i monitoringa rezultata

4. *Stručnjak* (ekspert) u zaštiti ima sledeća znanja, sposobnosti i veština:
   a. ima jaku želju i interes za sticanje znanja, veština i sposobnosti
   b. može izvršiti zadatke kontrole sistema zaštite bez posebnih priprema
   c. ima veliko iskustvo, može instruisati druge za izvršavanje zadataka
   d. veruje da može izvršiti zadatke kontrole, ali zahteva pomoć ili vreme za pripremu
5. *Profesionalac* u zaštiti ima sledeća znanja, sposobnosti i veština:
   a. ima jaku želju i interes za sticanje znanja, veština i sposobnosti
   b. može izvršiti zadatke kontrole sistema zaštite bez posebnih priprema
   c. ima veliko iskustvo, može instruisati druge za izvršavanje zadataka
   d. veruje da može izvršiti zadatke kontrole, ali zahteva pomoć ili vreme za pripremu
6. *Sposoban* u zaštiti ima sledeća znanja, sposobnosti i veština:
   a. ima jaku želju i interes za sticanje znanja, veština i sposobnosti
   b. može izvršiti zadatke kontrole sistema zaštite bez posebnih priprema
   c. ima veliko iskustvo, može instruisati druge za izvršavanje zadataka
   d. veruje da može izvršiti zadatke kontrole, ali zahteva pomoć ili vreme za pripremu
7. *Motivisan* u zaštiti ima sledeća znanja, sposobnosti i veština:
   a. ima jaku želju i interes za sticanje znanja, veština i sposobnosti
   b. može izvršiti zadatke kontrole sistema zaštite bez posebnih priprema
   c. ima veliko iskustvo, može instruisati druge za izvršavanje zadataka
   d. veruje da može izvršiti zadatke kontrole, ali zahteva pomoć ili vreme za pripremu
8. Tipični ciljevi uspostavljanja kapaciteta za kontrolu i reviziju zaštite IKTS su:
   a. obezbediti podršku za poboljšanje procesa planiranja zaštite
   b. podržati performanse procesa sertifikacije i akreditacije sistema zaštite
   c. dopuniti proces kontrole i revizije sa procenom efektivnosti sistema zaštite
   d. obezbediti nezavisnu kontrolu i reviziju za izradu politike zaštite
   e. podržati zahteve za korporacijsku digitalnu forenzičku istragu i analizu
   f. obezbediti podršku za sofisticiranu analizu i ekstrakciju podataka
   g. obezbediti mišljenje revizora zaštite u procesu razvoja sistema zaštite
9. Izveštaj o rezultatima revizije treba da sadrži:
   a. ciljeve, period rada, prirodu i obim izvršenih aktivnosti
   b. primenjene standarde, restrikcije, nalaze, zaključke i preporuke
   c. izmene plana i politike zaštite
   d. otkrivene informacije, koje mogu kompromitovati kontrolisani sistem
10. Glavni kriterijumi za ocenu rezultata revizije zaštite IKTS, za definisane strateške ciljeve, su:
   a. finansijska dobit
   b. poboljšanje sistema zaštite
   c. poboljšanje procesa zaštite
   d. poboljšanje metodologije zaštite

5. UPRAVLJANJE KOMPJUTERSKIM INCIDENTOM I VANREDNIM DOGAĐAJEM

Po završetku ovog poglavlja razumećete:

- Razliku između kompjuterskog događaja i incidenta
- Politiku, procedure i proces za upravljanje incidentom
- Glavne kategorije kompjuterskog incidenta
- Značaj planiranja i testiranja plana vanrednog događaja u IKTS
- Značaj izbora strategije za upravljanje VD
- Značaj pripreme rezervne lokacije i kapaciteta za oporavak IKTS

5.1. UVOD

Kompjuterski incident (KI), nastao zbog namernih malicioznih, *tehničkih aktivnosti* iznutra ili spolja, može imati nepredvidljive posledice i potrebno ga je kontrolisati. Definicija bezbednosnog KI je fleksibilna kod većine autora i varira, u zavisnosti od organizacije i IKTS okruženja. Za *reaktivne sisteme zaštite* rentabilno je razviti stacionarne kapacitete za brzo otkrivanje i reagovanje na KI. U *proaktivnom sistemu zaštite* znatno je veća verovatnoća sprečavanja štetnog uticaja KI. Većina bezbednosnih KI utiče na poslovanje organizacije. Najčešće, uticaj KI je relativno mali, a trajanje relativno kratko. Sa porastom zavisnosti poslovanja od IKTS, uticaj KI raste, a tolerancija na bilo kakve smetnje se smanjuje. Uticaj ili posledice KI, mogu se smanjiti na više načina. Upravljanjem kompjuterskim incidentom tesno je povezano sa planiranjem vanrednih događaja (VD), ali ga treba odvojeno planirati, da bi se smanjila kompleksnost upravljanja. Proces upravljanja KI obuhvata *uspostavljanje kapaciteta* i *upravljanje specifičnim tipovima KI*.

Planiranje VD uključuje više od samog planiranja evakuacije izvan zone u kojoj je uništen IKTS centar ili drugi kapaciteti organizacije. Plan obuhvata i kako neka organizacija održava kritične funkcije IKTS u operativnom stanju u vanrednim uslovima i nastavlja poslovanje. U većini kritičnih situacija za tipične poslovne IKTS, potrebno je uspostaviti lanac upravljanja i obezbediti svest menadžmenta o potrebi izgradnje kapaciteta organizacije za efikasno reagovanje na KI i VD. U kategoriju VD u IKTS, mogu se svrstati sve prirodne katastrofe, nestanak električnog napajanja, štrajkovi i odsustvo zaposlenih sa posla, kvarovi sistema za grejanje/hlađenje, opšti kvarovi opreme i dr. Ovi su događaji slučajni po svojoj prirodi i štetne posledice njihovog uticaja, mogu se smanjiti samo planiranjem, uspostavljanjem kapaciteta za upravljanje VD, uvežbavanjem scenarija VD i oporavkom sistema. Neke od brojnim napada, zloupotreba IKTS i posledica prirodnih događaja, mogu se fiksirati kroz standardne procedure administracije.

5.2. KOMPJUTERSKI DOGAĐAJ I KOMPJUTERSKI INCIDENT

Kompjuterski događaj je bilo koje uočljivo dešavanje i sistemski događaj, registrovan u log datoteci u RS/RM. *Kompjuterski incident* (KI) je događaj sa negativnim posledicama (pad RS, zagušenje saobraćaja RM, eskalacija privilegija i sl.). Upravljanje KI obuhvata sve događaje štetne za bezbednost IKTS. Definicija KI je evoluirala od *„bezbednosno relevantnog događaja koji dovodi do gubitka CIA informacija"*, do definicije u Internet okruženju – *„povreda ili imanentna pretnja za povredu i/ili primenu politike zaštite"* [45].

Kako su KI neizbežni i predstavljaju nepoznatu pretnju, zahteva se struktuirana procedura za kontrolu i upravljanje. Brojne tehničke specifikacije KI dostupne su na web lokacijama [29]. Svi KI nisu bezbednosno relevantni, pa je važno sa sigurnošću identifikovati izvor i prirodu KI. Generička podela incidenta je na one koji *ne predstavljaju glavnu pretnju* i one koji *mogu izazvati zaustavljanje poslova organizacije*. Važno je izvršiti pažljivu trijažu KI, po značaju za funkcionisanje poslovnog sistema. U procesu inicijalne istrage KI, treba pretpostaviti da je sistem zaštite probijen i utvrditi štetu. Program za upravljanje KI treba da uključuje definisanje adekvatnih mera zaštite, prioritete reagovanja i oporavka sistema. U praksi zaštite KI se retko na vreme prijavljuje, jer ga organizacije pokušavaju rešavati interno, sakriti od javnosti i sl. U određenim slučajevima, gde postoji očigledna šteta, kompromitacija ili zakonska odgovornost, izveštavanje o KI mora biti izuzetno brzo.

5.2.1. Politika i procedure za upravljanje incidentom

Politika za upravljanje KI, internim ili iznajmljenim kapacitetima, u većini organizacija obuhvata iste ključne elemente: *izjavu menadžera o angažovanju; namenu i ciljeve; obim i granice; identifikaciju prirode KI i posledica u kontekstu organizacije; strukturu, uloge i odgovornosti interventnog tima; način i formu izveštavanja; prioritete saniranja i metriku performansi kapaciteta za upravljanje KI.* Procedure za upravljanje KI detaljno objašnjavaju specifične aktivnosti procesa, tehnike, ček liste i formulare, koje koristi interventni tim. Pre distribucije, proceduru treba testirati i verifikovati, izvršiti obuku i pripremiti instrukciju za primenu. Kako se KI može dogoditi na bezbroj načina, nije praktično razvijati preciznu *korak–po–korak* proceduru [35, 45].

5.2.2. Kategorije bezbednosnog kompjuterskog incidenta

Generalno, organizacija se može pripremiti za upravljanje sa bilo kojim tipom KI, a specifično – sa poznatim tipovima. U praksi zaštite još uvek nema konsenzusa o najboljoj taksonomiji KI. Najčešća podela (nije konačna) je, na bazi primarnih kategorija

napada, na posledice: *odbijanja izvršavanja servisa, napada malicioznih programa, neovlašćenog pristupa, nepropisnog korišćenja IKTS i kombinovanih napada*. Neki KI mogu se svrstati u više od jedne kategorije. Ova podela je pre osnovno uputstvo za upravljanje KI [45, 72].

5.2.3. Nagoveštaji kompjuterskog incidenta

Glavni problem upravljanja KI je donošenje odluke da se incident dogodio, kojeg je tipa i intenziteta i kolika je šteta? Problem je tim teži, što KI tipično čini kombinacija raznih faktora (*KI mogu detektovati razna tehnička sredstva sa različitim nivoima tačnost/pouzdanosti, brojni su potencijalni znaci da se KI dogodio itd.)* i potrebno je specifično tehničko znanje i veliko iskustvo za analizu *nagoveštaja - predznaka* i *indikatora* KI [35].

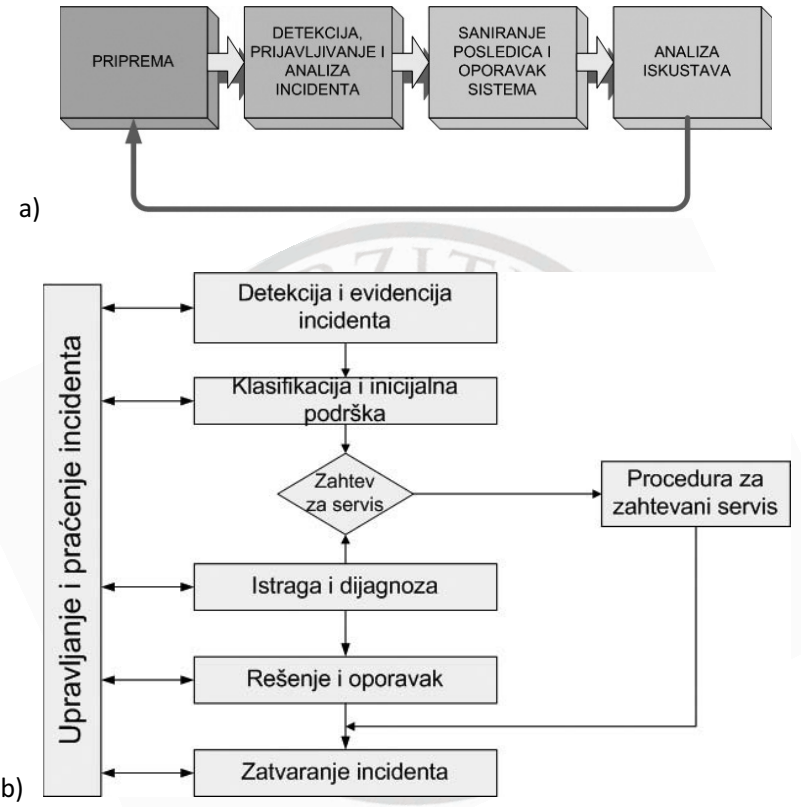
Predznak KI je nagoveštaj da se neki incident može dogoditi u bliskoj budućnosti, na primer: *log datoteka u web serveru pokazuje korišćenje skenera ranjivosti Web servera* itd. Svaki napad se ne može detektovati kroz predznake, neki napadi nemaju predznake, dok drugi – generišu predznake, koje organizacija ne uspeva detektovati. Ako se predznaci detektuju, organizacija ima priliku da izmeni sistem zaštite i spreči napad. *Indikator* KI je znak da se neki incident vrlo verovatno dogodio ili se upravo događa, na primer: *mrežni IDPS alarmira da je neki bafer preplavljen pokušajima napada na web server, AVP alarmira prisustvo virusa/crva, pad web servera* itd. Predznaci i indikatori KI identifikuju se iz više različitih izvora, od kojih su najčešći alarmi softverskih mehanizama zaštite RS/RM, log datoteke, javno raspoložive informacije i ljudi. Najčešći izvori indikatora i predznaka za svaku kategoriju KI, *kontrolne liste* za određivanje kategorije KI i analizu predznaka i indikatora, kao i generička procedura za upravljanje KI, dati su u literaturi [35, 45].

5.2.4. Upravljanje kompjuterskim incidentom

Cilj upravljanja KI je, da se ograniči mogućnost upada u sistem kroz *preventivnu zaštitu, testiranje otpornosti sistema na proboj, skeniranje ranjivosti sistema i IDPS,* kao i da se obezbedi lakši istražni postupak kada se incident dogodi. Životni ciklus upravljanja KI tipično ima četiri faze [35, 45, 72]: (1) *priprema, (2) detekcija, prijava i analiza, (3) saniranje posledica i oporavak sistema i (4) analiza iskustava* (Sl. 5.1a). Proces uptravljanja bezbednosnim KI prikazan je na slici 5.1.b.

U pripremnoj fazi uspostavljeni sistem zaštite i *interventni tim* – CIRT (*Computer Incident Response Team*) *preventivno* sprečavaju KI [7]. Primarni ciljevi razvoja kapaciteta za upravljanje KI su: (1) *reagovanje na KI*, (2) *saniranje štete* i (3) *oporavak sistema*. Kapaciteti za upravljanje KI, moraju biti preventivno implementirani i spremni da po potrebi obezbede: *brzo reagovanje, koordinaciju aktivnosti tima, izveštavanje o KI, opo-*

ravak sistema i sprečavanje ili minimizaciju potencijalne štete. Podaci o KI i korektivnim akcijama se skupljaju i skladište u bazu podataka i analiziraju za formiranje obrazaca ponašanja – *profil KI*, npr. najčešćeg tipa virusa i napadanog sistema, najbolje korektivne akcije.



Sl. 5.1. Životni ciklus - (a) i proces upravljanja bezbednosnim incidentom – (b)

Iako nije odgovoran za sprečavanje KI, CIRT čini glavnu komponentu kapaciteta za upravljanje incidentom. Ekspertska znanja članova tima dragocena su za poboljšanje sistema zaštite i dokazivanje zloupotrebe ili kompjuterskog kriminala. Članovi tima su tipično specijalisti za mrežnu tehniku, platforme i komunikacije i treba da su na raspolaganju 7x24 sata i fizički dostupni što je moguće brže; da imaju specifična znanja, veštine i sposobnosti za upotrebu neke tehnologije za upravljanje incidentom, digitalnu forenzičku istragu, akviziciju i analizu digitalnih podataka, timski rad i dobru komunikaciju sa različitim učesnicima. *Modeli struktura CIRT* za upravljanje KI mogu se svrstati u tri kategorije [57, 61]:

- *centralni CIRT,* koji upravlja KI u celoj organizaciji, efikasan je za male i veće organizacije sa malom distribucijom objekata IKTS;
- *distribuirani CIRT,* koji upravlja KI u logičnim ili fizičkim segmentima organizacije, kao deo jednog entiteta i procesa upravljanja;
- *koordinacioni CIRT,* koji savetodavno vodi rad drugog tima.

Tipičan *model popune CIRT* uključuje *interno zaposlene* sa ograničenom pomoći spolja, *delimično iznajmljene* usluge ili *potpuno iznajmljen tim* spoljnih saradnika. Dobri *kapaciteti* za upravljanje KI treba da poseduju nekoliko ključnih karakteristika: *razumevanje obima i granica procesa upravljanja i upotrebe kapaciteta, obrazovnu komponentu, sredstva za centralizovano upravljanje (komunikaciju i izveštavanje), specijaliste za primenjene tehnologije i dobre veze sa entitetima koji mogu pomoći u upravljanju KI*.

Obim i granice upotrebe kapaciteta za upravljanje KI ne obuhvataju uvek celu organizaciju. Kapaciteti za upravljanje KI obuhvataju tehnologiju, korisnike IKTS i menadžere. *Obuka* korisnika ima za cilj da se smanji kompleksnost, poveća korisnička prihvatljivost i obezbedi izveštavanje po prioritetima. *Centralizovano upravljanje* obezbeđuje efikasno i efektivno upravljanje KI, a uspeh zavisi od blagovremenog izveštavanja. Ako je KI hakerski napad, treba koristiti kriptozaštićen sistem za izveštavanje, analizu i čuvanje informacija o incidentu. *Tehnologija* za upravljanje KI treba da uključuje i specifične *forenzičke alate*. Većina CIRT formira prenosivi komplet za istragu kompjuterskog incidenta, u kojem se nalaze osnovni forenzički alati - laptop računar sa brojnim programima, uređaji za bekapovanje, čisti e-mediji, bazična oprema i kablovi za umrežavanje, mediji sa OS i aplikacijama [35].

U fazi detekcije i analize incidenta, kao osnovni alati, koriste se IDPS sistemi za detekciju i sprečavanje povrede sistema zaštite. Detektorski i preventivni alati obezbeđuju kontrolu neregularnih promena stanja u sistemu i obavljaju inicijalnu evaluaciju konfiguracije sistema. Prikupljaju informacije o napadu i napadaču, koje su korisne za forenzičku istragu i analizu. Dobro upravljanje upadom u IKTS, preventiva je svih potencijalnih problema i omogućava pokretanje istrage o KI. Međutim, IDPS sistemi proizvode veliki broj lažnih pozitiva, pa ne znači da se KI dogodio, čak i kada je neki indikator tačan. Pametno je sumnjati u svaki KI i smatrati da se događa, sve dok se ne pojave indikatori da se ne događa. Za efektivno upravljanje KI preporučuje se proces *korporacijske digitalne forenzičke istrage KI,* koji obuhvata faze *pripreme i podnošenja zahteva za istragu*, *akviziciju digitalnih dokaza, identifikaciju incidenta i napadača i forenzičko čuvanje i rukovanje digitalnim dokazima* [35].

Saniranje posledica KI i oporavak sistema uključuje razvoj metoda za saniranje posledica, najmanje od svih tipova glavnih kategorija KI. Za brže odlučivanje treba dokumentovati *kriterijume* za određivanje metoda za saniranje KI, koji uključuju: *potencijalna oštećenja i krađu objekata informacione imovine, obavezu čuvanja dokaza za forenzičku analizu i veštačenje, raspoloživost servisa, vreme i resurse potrebne za implementaciju*

metoda, efektivnost metoda (npr. sanira delimično ili potpuno) i *vreme trajanja rešenja* (npr. *hitno* – mora se ukloniti za četiri sata; *privremeno* – uklanja se za dve sedmice; *permanentno*) i dr. U fazi oporavka, treba eliminisati preostale komponente KI, izbrisati maliciozne kôdove i dezaktivirati probijene korisničke naloge. Faza oporavka može uključiti: *restauraciju sistema iz bekapa, zamenu kompromitovanih datoteka, instalaciju popravki, izmenu lozinki i povećanje zaštite perimetra RM, rekonfigurisanje sistema logovanja ili monitoringa RM i forenzičku analizu digitalnih podataka za otklanjanje pravog uzroka KI.*

Analiza iskustava, iako je najvažnija faza procesa upravljanja KI, često se zanemaruje, a uključuje: *tip i vreme KI, ponašanje menadžmenta i zaposlenih, dokumentaciju i adekvatnost procedura, potrebne informacije po izbijanju KI, preduzete akcije za sprečavanje i oporavak, iskustva za rad i korektivne akcije za sprečavanje budućeg, sličnog KI i potrebne resurse za detekciju, analizu i saniranje novog KI*. Mali incidenti ne zahtevaju posebnu analizu u ovoj fazi, osim ako ne otkrivaju nepoznati metod napada. Ako se dogodi ozbiljan napad, uvek je korisno izvršiti detaljnu multidisciplinarnu analizu [35].

Kompletiran izveštaj o analizi KI treba koristiti za *obuku, ažuriranje politike i dokumenata, popravku procedura, izradu pojedinačnih analitičkih izveštaja, izradu hronologije događaja iz log datoteka za dokazni postupak* itd. Na bazi normativnih zahteva, prethodnih izveštaja i očekivanja od sakupljenih podataka, organizacija odlučuje, koji se podaci o KI čuvaju. Treba sakupljati podatke, relevantne za upravljanje KI i dokazivanje pred sudom.

Podatke, koji se odnose na KI moguće je *meriti* na više načina: *broj saniranih KI, utrošeno vreme po KI, objektivna procena svakog KI, subjektivna procena svakog KI*, *periodična revizija programa za upravljanje KI i troškovi čuvanja i zadržavanje dokaza, koji* prema nacionalnom zakonu mogu biti: tipično – od jednog meseca do jedne godine, u slučaj sudskog procesa – do kraja procesa, podataka e-pošte – do sto osamdeset dana, a podataka o glavnom incidentu – do tri godine.

5.3. PLANIRANJE VANREDNIH DOGAĐAJA U IKTS

Planiranje VD i *kontinuiteta poslovanja* najsloženiji je deo posla. Kada organizacija odluči kako će nastavi poslovanje, primena plana je tada relativno lak zadatak. Proces planiranja VD obuhvata sledeće faze: (1) *identifikovanje funkcija IKTS,* kritičnih za kontinuitet poslovanja, (2) *identifikovanje resursa,* koji podržavaju kritične IKTS servise, (3) *procenu potencijalnih VD*, (4) *izbor strategije i (5) implementacija plana za upravljanja VD u IKTS* [15, 45].

(1) Identifikovanje funkcija IKTS kritičnih za misiju organizacije osnovni je preduslov za planiranje kontinuiteta poslovanja. Kriterijumi za određivanje kritičnosti misije/

poslovanja mogu biti bazirani na vremenu oporavka servisa IKTS, akumuliranom uticaju ili kombinaciji ovih faktora. Posebno je važno identifikovati i proceniti promene, koje VD može izazvati u vanradno vreme. Za većinu funkcija IKTS za podršku poslovanja dostiže se tačka u kojoj uticaj VD postaje toliko velik da su bespredmetni pokušaji održavanja kontinuiteta funkcija IKTS. Očigledno, kritične funkcije IKTS treba oporaviti, pre nego što se ova tačka dostigne. U procesu upravljanja VD, vreme je kritičan faktor i važno je što ranije identifikovati implikacije vremena na proces, kao i određivanje prioriteta saniranja posledica. Potpuna redundantnost za svaku kritičnu funkciju, skupa je za većinu organizacija. U slučaju katastrofe, određene IKTS funkcije neće se izvršiti. Ako se odrede prioriteti, povećava se sposobnost organizacije da preživi VD [45].

(2) Identifikovanje resursa, koji podržavaju kritične IKTS servise, uključujući i potrebno vreme za resurse – *stalno* ili *povremeno* – i uticaj neraspoloživosti resursa na misiju/poslovanje. Planiranje VD u IKTS treba da obuhvati sve resurse, koji su neophodni da se poslovni proces izvrši. Kada se dogodi VD u organizaciji neki uticaj se ispolji odmah i veoma je skupo sprečiti ga, ako ne i nemoguće. Veći broj uticaja događa se posle izvesnog vremena. Neki od ovih uticaja mogu se odložiti, preduzimanjem odgovarajućih akcija, neki sasvim otkloniti, a neki se ne mogu sprečiti. Definisanje neophodnih resursa za suzbijanje posledica VD treba da vrše ona lica koja znaju kako se izvršavaju servisi IKTS i kako objekti IKTS zavise od drugih resursa, kao i druge kritične zavisnosti, pošto svi resursi nisu kritični za izvršavanje najbitnijih poslovnih procesa. Često je neophodno formirati tim za planiranje VD, da bi se odredili potrebni resursi i razumeli kritični servisi IKTS, koje oni podržavaju. Tipičan tim uključuje izvršne, IKTS i glavne menadžere organizacije, a drugi članovi se pozivaju se po potrebi. Timom najčešće rukovodi koordinator za upravljanje VD, koga imenuje menadžment organizacije.

Problem je što menadžeri različito vide i identifikuju IKTS resurse ili previđaju interakciju svih resursa, koji podržavaju kritične poslovne procese, od kojih svi nisu čisti IKTS resursi. Potrebni resursi za podršku kritičnih servisa IKTS za planiranje VD mogu se svrstati u šest glavnih kategorija: *ljudi, kapaciteti za procesiranje, servisi, podaci i aplikacije, fizička infrastruktura i dokumentacija* [64, 35]:

1. *Ljudski resursi,* najvažniji za svaku organizaciju, obuhvataju administratore, specijaliste zaštite, operatere i korisnike.
2. *Kapaciteti IKTS za procesiranje* tradicionalno su prioritetni za planiranje VD. Iako je bekapovanje IKTS glavna aktivnost, važna su i alternativna rešenja.
3. *Aplikacije i podaci IKTS* su najkritičnija imovina, jer neposredno podržavaju misiju i tekuće poslovne procese organizacije.
4. *Servisi IKTS* podržavaju brojne poslovne procese, a najvažniji su *komunikacioni* (za prenos podataka) i *informacioni servisi* (*on-line* web servisi, e-trgovina, baze podataka, e-bilteni itd.).
5. *Fizička infrastruktura IKTS* obezbeđuje radno okruženje, odgovarajuću opremu i alate, neophodne za efektivan rad zaposlenih.

6. *Dokumentacija i e-evidencije*, koje podržavaju većinu servisa IKTS, mogu biti značajni i za legalne potrebe istrage kompjuterskog kriminala.

(3) Procena potencijalnih VD u IKTS i njihovih posledica prethodi razvoju scenarija šireg spektra VD. Scenario treba da uključi male i velike VD i važno je izbeći razvoj planova za svaki pojedinačni scenario VD. Tipičan scenario treba da uključi odgovore na pitanja za sve relevantne resurse [7, 35]:

1. *Ljudski resursi:* Mogu li zaposleni doći na posao? Koji zaposleni ima kritična znanja i veštine? Mogu li se zaposleni lako evakuisati na rezervnu lokaciju?
2. *Kapacitet za procesiranje:* Da li je IKTS ugrožen? Šta se događa ako neki od sistema nije u upotrebi? Postoji li lista prioritetnih akcija? Koje veze postoje?
3. *Aplikacije i podaci IKTS***:** Da li je ugrožen integritet podataka? Da li je neka aplikacija IKTS sabotirana? Može li neka aplikacija raditi na drugoj platformi?
4. *Servisi IKTS:* Može li IKTS komunicirati sa drugima i kojim sistemima? Mogu li ljudi komunicirati? Koliko dugo/često su IKTS servisi u prekidu? Mogu li se koristiti usluge iznajmljenih udaljenih transakcija?
5. *Fizička infrastruktura IKTS:* Imaju li zaposleni mesta, alate i opremu za rad? Mogu li zaposleni zaposesti zgradu za rad i da li postoji infrastruktura (voda, kanalizacija, ventilacija, grejanje, hlađenje)?
6. *Dokumentacija:* Mogu li biti pronađena potrebna elektronska dokumenta i da li su čitljiva?

(4) Izbor strategije za upravljanje VD: u evaluaciji rezervnih lokacija, potrebno je razmotriti koje su kontrole zaštite instalirane za sprečavanje i smanjenje uticaje VD na IKTS. Pošto ni jedan skup kontrola zaštite ne može rentabilno sprečiti sve potencijalne VD, u sistemu zaštite treba koordinirati preventivne mere za oporavak sistema. Glavna strategija svakog plana za upravljanje VD u IKTS treba da sadrži [3]:

1. *hitne intervencije* – inicijalne akcije za zaštitu ljudskih života i smanjenja štete;
2. *oporavak sistema* – akcije za obezbeđivanje kontinuiteta kritičnih funkcija i
3. *kontinuitet poslovanja* –povratak IKTS u normalni režim rada.

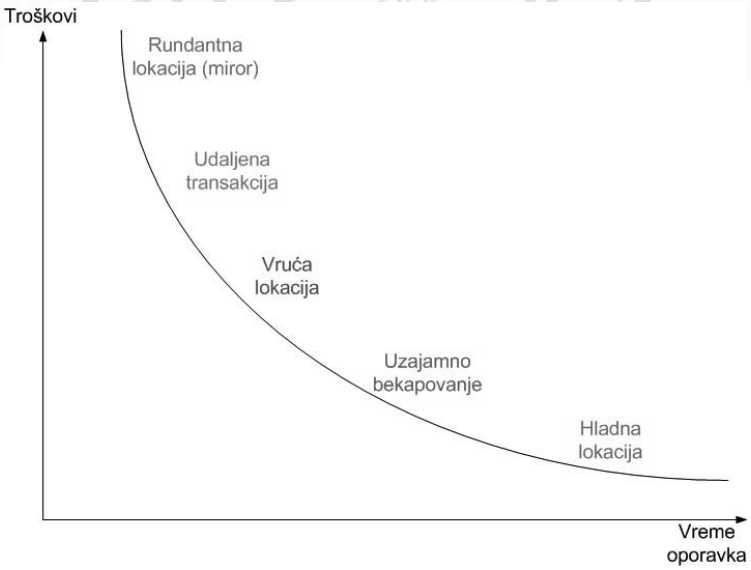
Odnos između oporavka i kontinuiteta rada IKTS je veoma važan. Što je duže potreban kontinuitet rada sistema, to će duže organizacija morati da radi u modu oporavljenog sistema. Oporavak sistema nije cilj sam po sebi, a kontinuitet normalnog rada sistema, uključujući povratak u rekonstruisanu ili novu lokaciju, uvek se mora dogoditi. Povratak i premeštanje operacija IKTS uvek izazivaju neke prekide. Faza povratka u normalni režim rada treba da bude uključena u sveobuhvatni plan za VD. Neke organizacije proces upravljanja VD dele na *hitne intervencije*, *operacije bekapovanja* i *oporavak sistem,* što nije presudno za uspešno upravljanje VD. Važno je da ove faze sadrže ozbiljan plan.

Izbor strategije zasniva se na praktičnoj analizi IKTS, uključujući izvodljivost i troškove. Za donošenje odluke o optimalnoj strategiji treba analizirati svaku od kategorija

resursa IKTS, opcije oporavka, rentabilnosti i rizika. Težište analize je na oblastima gde nije jasno koja je strategija najbolja [3]:

1. *Ljudski resursi,* u glavnom VD mogu biti pod značajnim stresom ili u panici. Ako je događaj regionalna nesreća, zaposleni prvo brinu za porodice i imovinu, neki ne mogu, a neki neće doći na posao, što znači da treba privremeno zaposliti nova lica. Ovo može uvesti rizik i treba ga uključiti u plan za VD.
2. *Kapaciteti za procesiranje IKTS* se grupišu u šest osnovnih kategorija [64]:
   - *primarna lokacija***:** postojeća zgrada opremljena sa IKTS kapacitetima;
   - *hladna lokacija:* prazna rezervna zgrada sa osnovnom infrastrukturom za smeštaj opreme IKTS, koja se lako može adaptirati u slučaju VD;
   - *vruća lokacija:* zgrada na rezervnoj lokaciji opremljena sa hardverom, softverom i mrežnom instalacijom, kompatibilnom sa primarnom;
   - *redundantna lokacija:* zgrada opremljena i konfigurisana potpuno jednako kao primarna;
   - *uzajamno bekapovanje:* recipročni ugovori za pomoć u slučaju VD; zahtevaju česta ažuriranja i održavanje kompatibilnosti konfiguracija IKTS;
   - *udaljena iznajmljena transakcija:* iznajmljena organizacija, koja po ugovoru vrši *online* periodično bekapovanje i oporavak u slučaju VD;
   - *hibridni sistemi:* bilo koja kombinacija gornjih kategorija.

Na Sl. 5.2. prikazani su troškovi oporavka sistema u funkciji rezervne lokacije. Očigledno je da troškovi rastu, ako se želi smanjiti vreme oporavka [45, 74].



Sl. 5.2. Dijagram troškova bekapovanja i vremena oporavka u funkciji rezervne lokacije

Sistem treba oporavljati prema redosledu zahteva za raspoloživost IKTS kapaciteta za procesiranje. Osnovni kapacitet za oporavak IKTS od VD je *bekapovanje* podataka i programa izvan primarne lokacije i korišćenje za oporavak IKTS.

3. *Za aplikacije i podatke* primarna strategija planiranja VD je regularno bekapovanje i skladištenje na alternativnu lokaciju. Važno je odrediti koliko često se vrši bekapovanje zavisi od *ažurnosti, upotrebne vrednosti* i *usklađenosti* podataka. U VD ostaje potreba za zaštitom IKTS, a u nekim slučajevima je i veća, na primer, zbog deljenja IKTS resursa, koncentracije više resursa u manjem prostoru ili angažovanja zaposlenih po ugovoru, koji nisu dovoljno bezbednosno provereni. U fazi oporavka sistema, oporavljeni podaci zastarevaju za vreme od poslednjeg bekapovanja do pojave VD. Da bi podaci bili korisni, moraju se češće bekapovati. Takođe, da bi oporavljeni IKTS funkcionisao, bitne su usklađenost i ažurnost bekapovanih podataka i sinhronizacija bekapovanih datoteka, uzetih sa različitih delova IKTS u različitim vremenima. U protivnom, mogu nastati problemi i sa restartovanjem računara sa poznatom konfiguracijom. Strategija bekapovanja IKTS treba da obezbedi oporavak sistema na najefikasniji način. Bekapovanje podataka, datoteka i aplikacija kritičan je deo svakog plana za VD [5].
4. *Servise IKTS za VD* mogu obezbediti i TTPS (telekomunikacioni, Internet) provajderi. Primarna lokacija je obično opremljena za prijem multimedija. Ako je jedan ISP izbačen iz rada, može se koristiti drugi. Značajno je identifikovati, koji je tip izgubljene komunikacije i da li je u pitanju lokalna ili udaljena veza. Lokalna telefonska veza se može prebaciti na mobilnu, ali je znatno teže prebaciti prenos velike količine podataka sa žične na bežičnu vezu. Takođe, nastavak normalnog rada sistema može zahtevati ponovno preusmeravanje komunikacionih servisa. Mehanizmi i servisi koji obezbeđuju visoku raspoloživost i otpornosti IKTS na otkaze predstavljaju preventivnu meru za kontinuitet poslovanja u slučaju VD. Primer tehnologije za visoku raspoloživost podataka su RAID (*Redundant Array of Independent Discs*) čvrsti diskovi, koji omogućavaju nastavak rada servera u slučaju kvara jednog diska, bez gubitaka podataka. Druga tehnologija je *klaster servera* koji deli klijentsko opterećenje i još bolje toleriše otkaze od RAID sistema. Ako otkaže jedan server, drugi preuzima i nastavlja rad. Naravno, ovi sistemi su od male koristi, ako su smešteni na istoj lokaciji. *Redundantne* servere treba razmestiti na alternativne lokacije i povezati u WAN mrežu. U slučaju prekida električnog napajanja, raspoloživost podataka, zavisno od kapaciteta, obezbeđuju i izvori neprekidnog napajanja – UPS (*Uninteruptable Power Suply*).
5. *Redundantna fizička infrastruktura* za VD, treba da bude planirana i ugovorena. Za premeštanje na rezervnu lokaciju, treba izraditi procedure za evakuaciju i povratak na primarnu ili novu lokaciju. Zaštita fizičke infrastrukture normalni je deo plana za hitne intervencije.
6. *Dokumentacija,* elektronska i papirna uključujući i arhivu, u primarnoj strategiji upravljanja VD obično se bekapuje na magnetske, optičke i druge medije i skladišti

na rezervnoj lokaciji. Papirnu dokumentaciju treba skladištiti na pristupačnoj alternativnoj lokaciji.

Kada se izabere strategija za upravljanje VD u IKTS, treba je dokumentovati i izvršiti pripremu i obuku.

(5) Implementacija plana za upravljanja VD u IKTS može zahtevati duge pripreme: uspostavljanje procedura za bekapovanje, sklapanje novih i obnavljanje postojećih ugovora za servise, nabavka IKTS opreme, ažuriranje servisa i opreme za bekapovanje, formiranje redundantnih kapaciteta, zamena dotrajale ili zastarele opreme, formalno pripisivanje odgovornosti itd. Važno je održavati pripremu ažurnom, uključujući i dokumentaciju. Za implementaciju plana je najznačajnije: *koliko scenarija i verzija plana treba razviti i ko priprema svaku verziju plana pojedinačno*?

Za male IKTS, plan za VD može biti deo plana zaštite. Za velike i kompleksne IKTS, plan zaštite može da sadrži kratak pregled plana za upravljanje VD, koji može biti poseban dokument. U centralizovanom upravljanju, najbolje je odrediti koordinatora za upravljanje VD, koji priprema plan sa ostalim menadžerima. *Dokumentovan plan za VD* mora biti ažurno održavan u skladu sa promenama i uskladišten na bezbedno mesto. Pisani dokument plana je kritičan faktor u VD i mora biti jasno napisan, razumljiv i na raspolaganju svim zaposlenim. Korisno je uskladištiti ažurne kopije na nekoliko lokacija, uključujući sve rezervne.

Obuka zaposlenih za VD obavezna je za sve zaposlene i novo-zaposlene. Povremeno treba izvoditi vežbe na kojima zaposleni praktično uvežbavaju svoje uloge u VD. Najvažnije su simulacije različitih scenarija prirodnih katastrofa i uvežbavanje ponašanja i postupaka zaposlenih. Obuka je posebno važna za efektivno reagovanje u hitnom slučaju. Testiranje plana za VD u IKTS treba vršiti periodično, jer plan vremenom zastareva, pa se moraju specifično dodeliti odgovornosti zaposlenim za održavanje ažurnosti plana. Testiranje uključuje *reviziju, analizu i simulaciju*.

Revizija može biti jednostavan test za proveru tačnosti dokumentacije plana, dostupnosti datoteka iz sistema za bekapovanje i poznavanja procedura za VD. *Analiza* se može izvršiti na celom ili delu plana, kao što su procedure za hitne resursa za podršku. Analitičari traže logične ili procesne slabosti i intervjuišu menadžere i druge zaposlene, da bi popravili plan. *Simulacija* krizne situacije i kako se transportuje na alternativnu lokaciju, što obezbeđuje informacije o greškama u planu za VD, kritične informacije za kontinuitet poslovanja i uvežbane procedure za realnu kriznu situaciju. Što je kritičnost funkcije za koju se simulira VD veća, tim je simulacija rentabilnija. Simulacija se može izvršiti sa rezervnom IKTS opremom za oporavak sistema (tzv. vrući test) ili na papiru (tzv. papirološki test) za proveru ljudi i plana.

Ova komponenta zaštite je praktično međuzavisna sa svim kontrolama zaštite, koje zajedno proaktivno sprečavaju VD u IKTS, a posebno sa *procenom rizika, fizičkom i personalnom zaštitom, upravljanjem kompujterskim incidentom i politikom zaštite***.** Troškovi razvoja i implementacije plana za VD u IKTS mogu biti značajni, zavisno od izbora strategije [45, 35].

5.4. REZIME

Kompjuterski incident je povreda ili imanentna pretnja za primenu politike zaštite. Na bazi primarnih kategorija napada, uobičajena je podela KI na *odbijanje izvršavanja servisa (DoS), napad malicioznih programa, neovlašćeni pristup i nepropisno korišćenje*. Generalno, postoji mnogo načina da organizacija redukuje uticaj ili ublaži posledice KI, preduzimanjem preventivnih mera za sprečavanje posledica KI. Kapaciteti za upravljanje KI obuhvataju *organizaciju i upravljanje specifičnim tipovima KI*.

Interventni tim za upravljanje incidentom – *centralni, distribuirani ili koordinirani*, može se popuniti sa zaposlenim, zaposlenim i spoljnim saradnicima i potpuno iznajmljenim članovima tima. Primarni ciljevi razvoja kapaciteta za upravljanje KI su *saniranje* štete i *oporavak* sistema, ali i za preventivno sprečavanja potencijalne štete, analizu rizika i obuku o zaštiti.

Nagoveštaji KI mogu biti *predznaci* da se neki incident može dogoditi i *indikator i*– da se incident vrlo verovatno dogodio ili se upravo događa. Nagoveštaji i indikatori se identifikuju iz više različitih izvora.

Proces upravljanja KI sadrži faze *pripreme*, *detekcije i analize*, *saniranja posledica i oporavak* i *analize iskustava*. Log datoteke IDPS su osnovni alati za prikupljanje informacija o napadu i napadaču za forenzičku istragu i analizu, saniranje KI i oporavak sistema. Nagoveštajima KI, ne može se uvek verovati zbog velikog broja netačnih indikacija.

Metod saniranja posledica KI varira u zavisnosti od kategorije i tipa. Preporučljivo je da se razvije poseban metod saniranja posledica za sve glavne tipove KI i da se kriterijumi za izbor odgovarajućeg metoda dokumentuju. Ovi kriterijumi mogu da uključe potencijalna oštećenja i krađu objekata, obavezu čuvanja dokaza za forenzičku analizu, raspoloživost servisa, vreme, resurse i efektivnost implementacije metoda i trajnost rešenja (hitno, privremeno, trajno). U toku analize iskustava iz upravljanja KI treba razmatrati brojna pitanja o prirodi incidenta, posledicama, načinu reakcije itd.

Plan za VD uključuje evakuaciju IKTS kapaciteta izvan ugrožene zone, način održavanja kritičnih servisa IKTS u operativnom stanju i oporavak sistema posle VD. Proces planiranja VD odvija se u šest faza. Za većinu servisa IKTS postoji tačka u kojoj uticaj VD postaje toliki, da su bespredmetni pokušaji održavanja kontinuiteta rada. U procesu upravljanja VD vreme je kritičan faktor, pa treba što ranije utvrditi uticaj vremena na proces i odrediti prioritet saniranja posledica.

Razvoj scenarija potencijalnih VD pomaže u razviju plana i treba da obuhvati *ljudske resurse, kapacitete za procesiranja, aplikacije i podatke, IKTS, infrastrukturu i dokumentaciju.* Neophodno je razmotriti koje su mere zaštite instalirane da spreče i smanje uticaj VD na IKTS i poslovanje. Potrebno je koordinirati preventivne mere i aktivnosti za oporavak sistema. Strategija planiranja i upravljanja VD u IKTS normalno sadrži *hitne intervencije, oporavak sistema i kontinuitet poslovanja*.

Plan za upravljanje VD mora biti napisan, ažurno održavan i uskladišten na bezbedno mesto. Svi zaposleni treba da prođu obuku za svoje uloge u VD. Implementacija strategije zaštite kritičnih IKTS servisa i resursa za podršku zahteva detaljnu pripremu tima za planiranje i upravljanje VD. Najznačajnije su izbor i broj scenarija, verzija planova i odgovornost lica za pripremu svakog plana. Plan vremenom postaje zastareo i treba ga periodično testirati i uvežbavati kroz *reviziju, analizu i simulaciju*.

Pošto sve kontrole zaštite proaktivno sprečavaju VD u IKTS, praktično postoje međuzavisnosti sa svim kontrolama, posebno analizom rizika, fizičkom i personalnom zaštitom, upravljanjem incidentom i politikom zaštite.

5.5. KLJUČNI TERMINI

Distribuiran DoS (DDoS): DoS tehnika koja koristi brojne hostove za izvršavanje napada.

Digitalna forenzika računara: sakupljanje, akvizicija i analiza kompjuterskih generisanih i uskladištenih digitalnih dokaza za potrebe forenzičke istrage; zahteva čuvanje integriteta digitalnih podataka u celom lancu istrage.

Incident: povreda ili imanentna pretnja promeni politike i standarda zaštite.

Interventni tim: ljudski kapaciteti uspostavljeni za upravljanje kompjuterskim incidentom.

Kapaciteti za upravljanje incidentom: Ljudi, tehnike i alati, metodi, vreme i drugi resursi na raspolaganju za upravljanje kompjuterskim incidentom.

Nagoveštaj: znak (predznak, indikator) da se neki incident može dogoditi ili se događa.

Odbijanje izvršavanja servisa (DoS**):** neki napad koji sprečava ili ometa ovlašćeno korišćenje servisa i informacija RM/RS iscrpljivanjem resursa.

Operacija bekapovanja: stvaranje rezervnih kopija za izvršavanje bitnih zadataka posle prekida rada IKTS i nastavljanje rada dok se objekti sistema ne oporave u dovoljnoj meri.

Oporavak (*Recovery***):** restauracija objekata IKTS i druge infrastrukture posle glavnog kompjuterskog incidenta.

Predznak: neki nagoveštaj da se napadač možda priprema da izazove incident.

Sistem za detekciju i sprečavanje upada u IKTS (IDPS): softverski (ili hardverski) alat koji otkriva sumnjive aktivnosti, alarmira administratora i potencijalno sprečava upad u IKTS.

Hitna intervencija: odgovor na hitni slučaj kao što su požar**,** poplava, prirodna katastrofa, teroristički napad i sl., da bi se zaštitili životi, ograničila šteta i smanjio uticaj na rad IKTS.

Hladna lokacija: prazan, rezervni objekat izvan lokacije organizacije, opremljen potrebnom infrastrukturom, pripremljenom za instalaciju IKTS opreme.

Kontinuitet poslovanja: aktivnosti održavanja kritičnih poslova u toku i posle VD.

Redundantna lokacija: lokacija opremljena sa IKTS, identičnim primarnom, sa bekapovanjem u rezervni sistem u realnom vremenu i transparentnim oporavkom.

Operacija bekapovanja: stvaranje rezervnih kopija programa i podataka za izvršavanje bitnih zadataka posle prekida rada, nastavljanje rada i potpun oporavak IKTS.

Oporavak: restauracija objekata IKTS posle glavnog oštećenja.

Plan kontinuiteta poslovanja: procedure i informacije razvijene, povezane i održavane u gotovosti za upotrebu u slučaju vanrednog događaja.

Uzajamno bekapovanje: dve organizacije sa sličnim konfiguracijama sistema obezbeđuju rezervne kopije jedna drugoj, za slučaj VD.

Vruća lokacija: lokacija sa hardverom, softverom i mrežnom instalacijom, koja je kompatibilna primarnoj instalaciji IKTS organizacije.

5.6. PITANJA ZA PONAVLJANJE

1. Koja mera je najpogodnija, kada NIDS sistem otkrije napadača na RM:
   a. pokušati identifikovati napadača
   b. sačuvati evidenciju u log datoteci bezbednosno relevantnih događaja
   c. izbrisati log datoteku i pokušati uhvatiti određene podatke ako se ponovi napad
   d. odštampati dnevnik rada i ostaviti kod portira za forenzičara
2. Kompjuterski događaj je:
   a. bilo koje uočljivo dešavanje u RS ili RM
   b. događaj sa negativnim posledicama
   c. sistemski događaj registrovan u log datoteci
   d. povreda ili pretnja za povredu i/ili primenu politike zaštite
3. Kompjuterski incident je:
   a. bilo koje uočljivo dešavanje u RS ili RM
   b. događaj sa negativnim posledicama
   c. sistemski događaj registrovan u log datoteci
   d. povreda ili pretnja za povredu i/ili primenu politike zaštite
4. Generička podela incidenta je na incidente koji:
   a. ne predstavljaju glavnu pretnju sistemu i organizaciji
   b. mogu izazvati zaustavljanje poslova organizacije
   c. mogu izazvati pad računarskog sistema i računarske mreže
5. Politika upravljanja kompjuterskim incidentom treba da sadrži sledeće elemente:
   a. izjavu menadžera o angažovanju, namenu, ciljeve, obim i granice
   b. identifikaciju incidenta i njegove posledice u kontekstu organizacije
   c. strukturu, uloge i odgovornosti menadžmenta organizacije
   d. zahtev za izveštavanje o svim/određenim tipovima incidenata
   e. prioritete saniranja incidenta i način i formu izveštavanja
   f. merenje performansi kapaciteta za upravljanje rizikom
6. Podela incidenta na bazi primarnih kategorija napada je na:
   a. odbijanje izvršavanja servisa (DoS/DDoS),
   b. krađa identiteta i prisluškivanje
   c. napad malicioznim programom
   d. neovlašćeni pristup i nepropisno korišćenje IKTS
   e. kombinovani napad
7. Predznaci incidenta mogu biti:
   a. log datoteka u Web serveru pokazuje korišćenje skenera ranjivosti
   b. veliki broj povezanih e–*mail*–ova sa sumnjivim sadržajem
   c. neobična odstupanja od tipičnog mrežnog toka
   d. najavljena nova iskoristivost koja pogađa ranjivost servera e–pošte
   e. neovlašćen pristup web servisima na Internetu i preteće e–*mail* poruke
   f. pretnja grupe hakera da će napasti organizaciju
   g. mrežni IDPS alarmira da je neki bafer web servera preplavljen
   h. antivirusni program alarmira prisustvo virusa/crva u računaru
   e. pad web servera i promena *auditing* konfiguracije u log datoteci hosta
   f. više neuspelih pokušaja udaljenog pristupa nepoznatog korisnika u log datoteci
8. Indikatori incidenta su:
   a. log datoteka u Web serveru pokazuje korišćenje skenera ranjivosti
   b. veliki broj povezanih e–*mail*–ova sa sumnjivim sadržajem
   c. neobična odstupanja od tipičnog mrežnog toka
   d. najavljena nova iskoristivost koja pogađa ranjivost servera e-pošte
   e. neovlašćen pristup web servisima na Internetu i preteće e-*mail* poruke
   f. pretnja grupe hakera da će napasti organizaciju

g. mrežni IDPS alarmira da je neki bafer web servera preplavljen
h. antivirusni program alarmira prisustvo virusa/crva u računaru
i. pad web servera i promena *auditing* konfiguracije u log datoteci hosta
j. više neuspelih pokušaja udaljenog pristupa nepoznatog korisnika u log datoteci

9. Članovi tima za upravljanje KI (CIRT) treba da poseduju:
   a. ekspertska znanja i sposobnost za timski rad
   b. specifične veštine za upravljanje nekom tehnologijom zaštite
   c. specifične veštine za digitalnu forenzičku istragu
   d. dobre komunikacione sposobnosti
   e. da su povremeno na raspolaganju
10. Proces korporacijske digitalne forenzičke istrage KI uključuje:
    a. pripremu i podnošenje zahteva za istragu kompjuterskog incidenta
    b. akviziciju i rukovanje sa digitalnim dokazima
    c. identifikaciju incidenta i napadača
    d. ulazak u trag napadaču i hapšenje
    e. forenzičko rukovanje sa digitalnim dokazima kao da će biti predati sudu
11. Podatke koji se odnose na incidente moguće je meriti na bazi:
    a. broja saniranih incidenata u određenom vremenskom periodu
    b. utrošenog vremena za planiranje otklanjanja posledica incidenta
    c. utrošenog vremena za otklanjanje uzroka i posledica incidenta
    d. subjektivne procene rizika i revizije programa za upravljanje rizikom
    e. objektivne analize i procene uzroka i prirode svakog incidenta
    f. zadržavanje dokaza o incidentu u proizvoljnom vremenskom periodu
    g. finansijskog gubitka i druge štete koju je incident izazvao
12. Glavne faze procesa upravljanja kompjuterskim incidentom (KI) su:
    a. priprema, detekcija, prijavljivanje, analiza predznaka
    b. detekcija, prijavljivanje, analiza incidenta i saniranje posledica
    c. formiranje tima za upravljanje incidentom
    d. saniranje posledica i oporavak sistema, analiza iskustava
    e. analiza i profilisanje napadača
13. Proces planiranja vanrednih događaja (VD) obuhvata sledeće faze:
    a. identifikaciju funkcija IKTS kritičnih za kontinuitet poslovanja
    b. identifikovanje resursa koji podržavaju kritične IKTS servise
    c. procenu potencijalnih vanrednih događaja
    d. izbor strategije za upravljanje rizikom
    e. implementacija plana za upravljanje rizikom
    f. implementacija plana za upravljanja VD u IKTS
14. Glavni resursi potrebni za upravljanje VD su:
    a. ljudski resursi
    b. kapaciteti IKTS za procesiranje
    c. serveri
    d. aplikacije i podaci IKTS
    e. servisi IKTS
    f. fizička infrastruktura IKTS
    g. dokumentacija poslovnih procesa
    h. dokumentacija IKTS
15. Sredstva za podršku rada IKTS, kao što je električno napajanje, obično nisu uneta u plan za VD i kontinuitet poslovanja, zato što su:
    a. veoma pouzdana
    b. skupa za održavanje
    c. teška za upravljanje
    d. nije tačno ni jedno od navedenih
16. Upravljanje vanrednim događajem i kontinuitetom poslovanja je:
    a. proces, koji se obavlja u organizaciji i koji obuhvati sve odseke i nivoe
    b. proces odseka za IKTS, odgovornog za rad IKTS

c. u slučaju VD svaki rukovodilac odseka mora da napravi zaseban plan za VD
d. projekat vlade, koja organizacijama diktira pripremne zahteve za VD

18. Glavna (primarna) lokacija je:
a. zgrada na rezervnoj lokaciji opremljena sa hardverom, softverom i mrežnom instalacijom, kompatibilnom primarnoj mrežnoj instalaciji IKTS
b. iznajmljena organizacija po ugovoru, koja vrši *online* transmisiju podataka radi periodičnog bekapovanja i oporavka sistema
c. postojeća zgrada opremljena sa IKTS kapacitetima
d. prazna rezervna zgrada sa osnovnom infrastrukturom za smeštaj IKTS opreme, koja se lako može adaptirati u slučaju vanrednog događaja
e. bilo koja kombinacija gornjih kategorija
f. *miror* lokacija opremljena i konfigurisana potpuno jednako kao primarna
g. sporazum, plan i održavanje kompatibilnosti konfiguracija IKTS i aplikacija

19. Hladna lokacija je:
a. zgrada na rezervnoj lokaciji opremljena sa hardverom, softverom i mrežnom instalacijom, kompatibilnom primarnoj mrežnoj instalaciji IKTS
b. iznajmljena organizacija po ugovoru, koja vrši *online* transmisiju podataka radi periodičnog bekapovanja i oporavka sistema
c. postojeća zgrada opremljena sa IKTS kapacitetima
d. prazna rezervna zgrada sa osnovnom infrastrukturom za smeštaj IKTS opreme, koja se lako može adaptirati u slučaju vanrednog događaja
e. bilo koja kombinacija gornjih kategorija
f. *miror* lokacija opremljena i konfigurisana potpuno jednako kao primarna
g. sporazum, plan i održavanje kompatibilnosti konfiguracija IKTS i aplikacija

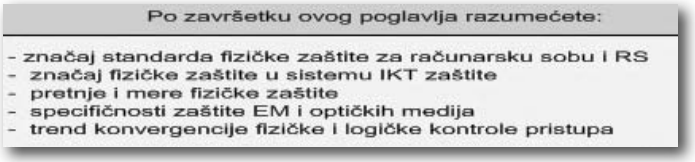
20. Vruća lokacija je:
a. zgrada na rezervnoj lokaciji opremljena sa hardverom, softverom i mrežnom instalacijom, kompatibilnom primarnoj mrežnoj instalaciji IKTS
b. iznajmljena organizacija po ugovoru, koja vrši *online* transmisiju podataka radi periodičnog bekapovanja i oporavka sistema
c. postojeća zgrada opremljena sa IKT kapacitetima
d. prazna rezervna zgrada sa osnovnom infrastrukturom za smeštaj IKTS opreme, koja se lako može adaptirati u slučaju vanrednog događaja
e. bilo koja kombinacija gornjih kategorija
f. *miror* lokacija opremljena i konfigurisana potpuno jednako kao primarna
g. sporazum, plan i održavanje kompatibilnosti konfiguracija IKTS i aplikacija

21. Redundantna lokacija je:
a. zgrada na rezervnoj lokaciji opremljena sa hardverom, softverom i mrežnom instalacijom, kompatibilnom primarnoj mrežnoj instalaciji IKTS
b. iznajmljena organizacija po ugovoru, koja vrši *online* transmisiju podataka radi periodičnog bekapovanja i oporavka sistema
c. postojeća zgrada opremljena sa IKTS kapacitetima
d. prazna rezervna zgrada sa osnovnom infrastrukturom za smeštaj IKTS opreme, koja se lako može adaptirati u slučaju vanrednog događaja
e. bilo koja kombinacija gornjih kategorija
f. *miror* lokacija opremljena i konfigurisana potpuno jednako kao primarna
g. sporazum, plan i održavanje kompatibilnosti konfiguracija IKTS i aplikacija

22. Uzajamno bekapovanje je:
a. zgrada na rezervnoj lokaciji opremljena sa hardverom, softverom i mrežnom instalacijom, kompatibilnom primarnoj mrežnoj instalaciji IKTS
b. iznajmljena organizacija po ugovoru, koja vrši *online* transmisiju podataka

radi periodičnog bekapovanja i oporavka sistema
   c. postojeća zgrada opremljena sa IKT kapacitetima
   d. prazna rezervna zgrada sa osnovnom infrastrukturom za smeštaj IKTS opreme, koja se lako može adaptirati u slučaju vanrednog događaja
   e. bilo koja kombinacija gornjih kategorija
   f. *miror* lokacija opremljena i konfigurisana potpuno jednako kao primarna
   g. sporazum, plan i održavanje kompatibilnosti konfiguracija IKTS i aplikacija
   h. recipročni ugovori koji dopuštaju da se IKTS organizacija međusobno pomognu u slučaju VD i koji zahtevaju često ažuriranje
23. Udaljena iznajmljena transakcija je:
   a. zgrada na rezervnoj lokaciji opremljena sa hardverom, softverom i mrežnom instalacijom, kompatibilnom primarnoj mrežnoj instalaciji IKTS
   b. iznajmljena organizacija po ugovoru, koja vrši *online* transmisiju podataka radi periodičnog bekapovanja i oporavka sistema
   c. postojeća zgrada opremljena sa IKTS kapacitetima
   d. prazna rezervna zgrada sa osnovnom infrastrukturom za smeštaj IKTS opreme, koja se lako može adaptirati u slučaju vanrednog događaja
   e. bilo koja kombinacija gornjih kategorija
   f. *miror* lokacija opremljena i konfigurisana potpuno jednako kao primarna
   g. sporazum, plan i održavanje kompatibilnosti konfiguracija IKTS i aplikacija
24. Hibridni sistemi bekapovanja su:
   a. zgrada na rezervnoj lokaciji opremljena sa hardverom, softverom i mrežnom instalacijom, kompatibilnom primarnoj mrežnoj instalaciji IKTS
   b. iznajmljena organizacija po ugovoru, koja vrši *online* transmisiju podataka radi periodičnog bekapovanja i oporavka sistema
   c. postojeća zgrada opremljena sa IKTS kapacitetima
   d. prazna rezervna zgrada sa osnovnom infrastrukturom za smeštaj IKTS opreme, koja se lako može adaptirati u slučaju VD
   e. sporazum, plan i održavanje kompatibilnosti konfiguracija IKTS i aplikacija
   f. *miror* lokacija opremljena i konfigurisana potpuno jednako kao primarna
   g. bilo koja kombinacija gornjih kategorija
25. Ključne vrste testiranja plana za vanredni događaj su:
   a. analiza, sinteza i simulacija
   b. revizija, analiza i simulacija
   c. revizija, obuka i simulacija

6. UPRAVLJANJE FIZIČKO-TEHNIČKOM ZAŠTITOM



6.1. UVOD

Fizička zaštita i zaštita okruženja IKTS treba da se zasnivaju na standardima i principima dobre prakse fizičke zaštite značajnih objekata, koja uključuje fizičko obezbeđenje i tehničku zaštitu - video nadzor, PPZ i protiv-provalnu zaštitu (3PZ).

U pristupu fizičkoj zaštiti IKTS, treba primenjivati standardne principe fizičke zaštite kao što su zaštita po dubini, planiranje lokacije, akomodacija, redovan nadzor i revizija zaštite, zaštita zaposlenih i klijenata, upravljanje VD, fizička zaštita klasifikovanih informacija i fizičkih objekata IKTS, konzistentnost i specifičnost fizičke zaštite RS/RM i zaštite papirnih informacija i medija za masivno skladištenje.

6.2. STANDARDI FIZIČKE ZAŠTITE

6.2.1. Standardi fizičke zaštite za računarsku sobu i radne stanice

U procesu upravljanja fizičkom zaštitom IKTS treba koristiti raspoložive nacionalne standarde za fizičku zaštitu značajnih objekata, fizičku zaštitu *računarske sobe* i *radne stanice*, koje izdaje nacionalno telo za standardizaciju. Ovi standardi obuhvataju fizičku zaštitu klasifikovanih i neklasifikovanih objekata. Klasifikovani objekti sadrže *restriktivne zone* i standardi nisu dostupni, a za neklasifikovane su javno dostupni. Klasifikovani standardi uključuju video nadzor i značajniju 3PZ. Standardi za fizičku zaštitu radnih stanica su uključeni u standarde računarske sobe, a mera fizičke zaštite se rangira obično na 4 nivoa - od najvišeg (4) do najnižeg (1) [2]**.** Zaštita fizičke infrastrukture je od presudnog značaja za zaštitu RM i IKTS u celini i čini osnovu na kojoj se izgrađuje sistem zaštite RM OSI modela [69].

6.3. FIZIČKA ZAŠTITA I ZAŠTITA OKRUŽENJA IKTS

6.3.1. Rizici proboja fizičke zaštite i zaštite okruženja IKTS

Termin *fizička zaštita* i *zaštita okruženja* IKTS odnosi se na mere i metode fizičke zaštite objekata IKTS, zgrada i infrastrukture okruženja za podršku rada IKTS, od slučajnih ili namernih pretnji, a obuhvata sledeće tri ključne oblasti [35, 34, 41]:

1. *fizičke objekte*: zgrade, građevinske strukture, vozila sa RS i dr.
2. *operativnu lokaciju:* određenu na bazi prostornih karakteristika *prirodnih i humanih pretnji* i *sekundarnih oštećenja* (eksplozija, vatra itd.).
3. *okruženje IKTS*: servisi za podršku rada IKTS (napajanje, grejanje, hlađenje i telekomunikacije), čiji nestandardan rad može izazvati prekid rada IKTS.

Fizička zaštita IKTS i okruženja obezbeđuje i zaštitu zaposlenih, a težišno je usmerena na zaštitu IKTS od sledećih pretnji:

- *prekida izvršavanja servisa* (*DoS*): veličina štete zavisi od trajanja prekida servisa i karakteristike operacije i korisnika akcija;
- *fizičkih oštećenja* hardvera i softvera IKTS: mogu se popraviti ili zameniti; veličina štete zavisi od cene popravke/zamene i troškova prekida servisa;
- *neovlašćenog otkrivanje informacija*: fizička ranjivost prostorija za smeštaj IKTS; posebno opasno u visoko distribuiranom mrežnom okruženju;
- *gubitka kontrole integriteta IKTS:* može izazvati napadač koji dobije fizički pristup serveru/računaru; posledice mogu biti krađa/prekid servisa, otkrivanje i izmena informacija, pronevera itd; teško je odrediti šta je modifikovano, izbrisano ili korumpirano; značajni su troškovi zamene ukradenog hardvera i restauracije podataka, a troškovi nastali zbog otkrivanja osetljivih informacija mogu biti nepredvidljivo veliki.

6.3.2. Fizička zaštita IKTS i okruženja

Fizička zaštita IKTS i okruženja obuhvata kontrolu fizičkog pristupa perimetru i ulazu u zgradu i u restriktivne prostore u zgradi, proces fizičke identifikacije zaposlenih (bedževi, kartice), podsisteme za grejanje, hlađenje i ventilaciju, 3PZ, video nadzor, zaštitu EM i optičkih medija i komunikacija. Mere fizičke zaštite IKTS i okruženja grupišu se u osam oblasti [41]: *barijere za fizički pristup, PPZ zaštita, sistemi za grejanje, hlađenje i ventilaciju, kolaps fizičke strukture, vodovodne instalacije, prisluškivanje podataka, uticaj EM smetnji i mobilne sisteme.*

Barijera za fizički pristup ograničava ulaz/izlaz personala, opreme i medija u/iz zone zaštite, a uključuje *restriktivni prostor*, *barijeru za opštu izolaciju, ulaznu tačku u bari-*

jeri i mere zaštite ulazne tačke. Zaposleni u restriktivnim prostorima IKTS igraju važnu ulogu u fizičkoj zaštiti, jer kontrolišu sva nepoznata lica. Barijere za fizički pristup štite restriktivne zone sa objektima IKTS, lokacije kabliranja i električnog napajanja, sisteme za hlađenje i grejanje, telefonske i linije za prenos podataka, kao i druge elemente potrebne za rad IKTS. U slučaju životne opasnosti u VD, prednost treba dati izlazima za slučaj opasnosti, ali je moguće izbalansirati oba zahteva (npr. bravom sa vremenskim kašnjenjem).

Postoji više vrsta barijera za fizički pristup, uključujući fizičko obezbeđenje, bedževe, memorijske kartice, ključeve, pokretna vrata, ograde i vrata sa šifrovanom bravom. Treba analizirati efektivnost barijera za fizički pristup u radno i vanradno vreme, kao i izvodljivost tajnog ulaska. Dodavanjem višeslojnih barijera, može se smanjiti rizik neovlašćenog ulaska u zonu zaštite. Video nadzor i 3PZ detektori kretanja i drugi senzori mogu detektovati i alarmirati ulaske u *restriktivne* prostore i fizički pristup objektima IKTS.

Protiv-požarna zaštita (PPZ) u zgradi posebno je značajna za bezbednost IKTS, zbog rizika za ljudske živote, potencijalnog uništenja hardvera, softvera i podataka i druge štete od požara. Faktori rizika od požara za objekte IKTS su [35]:

- *izvori požara,* materije koje emituju dovoljnu toplotu koja može izazvati paljenje drugih materijala;
- *izvori goriva* i kiseonik moraju postojati za održavanje i širenje požara; više sagorivog materijala po kvadratnom metru, znači veći požar i veću štetu;
- *ispravno održavanja zgrade***,** posebno PPZ sistema, minimizira akumulaciju sagorivog materijala, a time i rizik od izbijanja požara;
- *sadržaj zgrade* sa iznad-prosečnim brojem potencijalnih izvora požara (npr. skladište lako zapaljivih meterijala) inherentno je opasniji od drugih;
- *detektori požara,* što su brži, lakše će se i brže ugasiti požar i smanjiti ukupna šteta; vrlo je važno precizno odrediti mesto izbijanja požara;
- *PPZ aparati* za gašenje vatre mogu biti *automatski* (npr. raspršivači vode) ili *poluautomatski* (npr. klasični pokretni PPZ aparati), namenjeni za gašenje električnih instalacija i elektronske opreme i propisno održavani.

Kvarovi tehničkih uređaja za obezbeđenje radnog okruženja IKTS smanjuju tehničku pouzdanost sistema. Kvarovi sistema za grejanje/hlađenje, obično izazivaju prekid servisa IKTS i mogu oštetiti hardver. *Tehnička pouzdanost* tih sistema određuje se na osnovu faktora **MTBF** (srednje vreme između otkaza) i **MTBR** (srednje vreme između popravki–remonta) za električnu centralu, toplanu, pumpnu stanicu za snabdevanje vodom, sistem za ventilaciju i kanalizaciju i druge pomoćne sisteme za rad IKTS i konfor radnog osoblja. Rizik se može smanjiti zamenom uređaja sa nižim MTBF ili instalacijom redundantnih sistema, skladištenjem rezervnih delova i obukom osoblja za održavanje sistema [35].

Kolaps zgrade zbog zemljotresa, snežne lavine, klizišta, oluje, eksplozije ili požara, odnosi se, pre svega, na visoke, prostrane zgrade bez nosećih stubova.

Kvarovi vodovodnih instalacija mogu biti veoma razorni. Plan zgrade pomaže da se lociraju vodovodne instalacije, rizične za hardver IKTS. Lokacija sigurnosnih ventila i korisničke procedure moraju biti precizne i trenutno dostupne.

Prisluškivanje podataka, zavisno od tipa podataka i procesa IKTS, može nositi značajan rizik. Postoje tri načina presretanja (*intercepcije*) podataka u IKTS:

- *direktno osmatranje* monitora radnih stanica od strane neovlašćenih lica, što je u većini slučajeva lako je sprečiti premeštanjem monitora.
- *intercepcija transmisije podataka* na fizičkim linijama lokalne mreže, omogućava prisluškivanje, čitanje/snimanje paketa podataka, u aktivnom ili pasivnom režimu. Kod bežičnih mreža mogućnost intercepcije se povećava.
- *elektromagnetska intercepcija* koristi parazitno ili kompromitujuće zračenje EM energije (KEMZ), koje emituju, kondukcijom i radijacijom, svi aktivni uređaji i mrežne instalacije IKTS. Ovo zračenje može se detektovati sa specijalnim prijemnicima i antenama, a uspeh zavisi od snage signala, osetljivosti i lokacije prijemnika i antenskog sistema. Tehnologija za EM intercepciju KEMZ signala naziva se TEMPEST (*Transient Elektro–Magnetic Pulse Surveillance Technology*), kao i standard za zaštitu od KEMZ-a – TEMPEST (*Transient Elektro Magnetic Pulse Emanating Standard*), koji definiše oklapanje uređaja, računarske sobi ili cele zgrade i druge načine smanjenja širenja KEMZ signala [74, 77, 34]. TEMPEST otporne računare i perifernu oprema uglavnom koriste državne organizacije [35].
- *EM interferencija*, takođe, može predstavljati rizik za sistem zaštite i IKTS. Postoji nekoliko tipova spoljnih EM interferencija. *EM indukcija* od munje može na energetskoj ili komunikacionoj liniji izazvati potencijalno opasnu indukciju EM energije i kvar uređaja. *Statičko pražnjenje* može izazvati energetsko preopterećenje, oštetiti čipove i štampana kola i usporiti kretanja mehaničkih delova, čak i ispod nivoa detekcije. *EM interferencije (EMI*) sa spoljnim izvorima električne emisije, mogu izazvati brisanje podataka, korupciju datoteka i prekid rada lokalne opreme. *Radio–frekvencijska interferencija (RFI)* može izazvati korupciju i brisanje podataka i oštećenja opreme, koja ne može prepoznati komande iz legitimnog izvora.

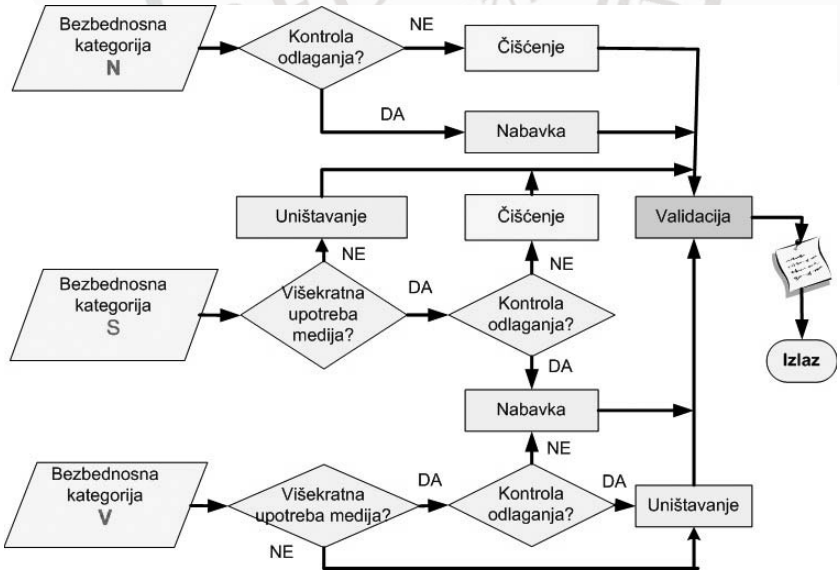
Mobilni i prenosni sistemi, instalirani u vozilu ili prenosni (*Lap Top, Noutbook*), obično zahtevaju modifikaciju analize i procene rizika. Računarski sistem u vozilu deli iste rizike kao i samo vozilo, uključujući udese i krađu, kao i regionalne i lokalne faktore rizika. Portabl sistemi imaju veći rizik od krađe i fizičkog oštećenja, a osetljive ili važne podatke treba uskladištiti na pokretni medij ili šifrovati. Dodatnu zaštitu obezbeđuju hardverski i/ili softverski uređaji za kontrolu pristupa.

6.3.3. Zaštita EM i optičkih medija

Generalno, postoji oprema koja može kompletno ukloniti sve magnetske tragove sa odloženih EM medija, uključujući RAM memorije. Pri tome treba razlikovati procese

saniranja i *deklasifikacije* medija. *Saniranje* je proces brisanja, što je moguće više podataka sa medija ili računarske opreme, koji ne uništava i ne menja automatski klasifikaciju medija/opreme. *Deklasifikacija* je uklanjanje ili redukcija nivoa klasifikacije medija/opreme na bazi procene rizika, odluke o otkrivanju preostalih podataka, procene ugovornih obaveza i eventualne prodaje, odlaganja i popravke opreme. Mediji/oprema koji nose klasifikovane podatke, moraju imati oznaku najvećeg stepena klasifikacije podataka, dok se ne izvrši propisano saniranje ili deklasifikacija. Magnetni mediji se deklasifikuju *demagnetizacijom* i *višestrukim presnimavanjem* [2].

Demagnetizacija smanjuje gustinu magnetnog fluksa primenom reverznog magnetnog polja i obezbeđuje nečitljivost prethodno snimljenih podataka i informacija. *Višekratno presnimavanje* magnetnih medija uzastopnim binarnim 1 i 0, standardno se koristi za efikasno brisanje podataka. Ciklus se ponavlja više puta, zavisno od procenjenog rizika ili zahteva za deklasifikaciju, a preporučuju se sledeći koraci: (1) *presnimiti sve lokacije bita podataka sa binarnom 0 i proveriti uspeh, (2) presnimiti sve lokacije bita podataka sa binarnom 1 i (3) proveriti uspeh i ponoviti 1. i 2. korak više puta prema zahtevu za deklasifikaciju ili proceni rizika*. Nepotpuno izbrisani i neispravno klasifikovani mediji/uređaji koji se ne mogu sanirati demagnetizacijom i višestrukim presnimavanjem, moraju se fizički uništiti. *Laserski štampači i kopir aparati* mogu se sanirati i deklasifikovati štampanjem praznih kopija, nakon poslednjeg štampanja klasifikovanih informacija. Proces saniranja i odlaganja dokumenata i medija prikazan je na Sl. 6.1.



Sl. 6.1. Tok procesa saniranja i odlaganja dokumenata i medija

Procedura zaštite EM i optičkih medija treba da specifično obuhvati mere zaštite od otkrivanja poverljivih informacija sa odloženih, neispravnih ili zastarelih medija/opreme i fizičku zaštitu korišćenih arhiviranih medija. *Memorijski čipovi* i drugi elementi za skladištenje saniraju se ili deklasifikuju na bazi procene rizika, uklanjanjem izvora napajanja i uzemljivanjem memorijskih elemenata. Međutim, u razvoju su *holografske* tehnologije za skladištenje informacija i *molekularna* memorija, za koje tek predstoji razvoj adekvatnih mehanizama za saniranje.

Hologramska memorija skladišti podatke na hologramsku 3D sliku, propuštanjem svetlosti kroz svetlosno osetljivi kristal, koji zadržava optički obrazac. Ima nekoliko hiljada puta veći kapacitet i nema mehaničke delove. Velika količina podataka čita se i upisuje jednostavnim komandama *čitaj* ili *piši*, nasuprot današnjim 2D memorijama, koje čitaju i upisuju podatke bit po bit. Sistem za *hologramsko skladištenje* može uskladištiti na hiljade stranica (blokova) podataka, sa preko milion bita svaka. Zauzima prostor veličine kocke šećera, npr. 10 GB podataka staje u 1 cm^3. Brzina pristupa podacima dostiže 1 Gbps, pošto memorija nema mehaničkih delova, a podacima (stranicama) se pristupa paralelno.

Molekularna memorija skladišti podatke koristeći protein *bakteriorodopsin* (*bacteriorhodopsin*). Neki laser može izmeniti protein iz stanja R (binarna **0**) u stanje Q (binarna **1**), što ga čini idealnim **ILI** ili *flip–flop* kolom za skladištenje binarnih podataka. Memorija je jeftina za proizvodnju i može raditi u većem temperaturnom opsegu nego poluprovodnička. Promena molekularnog stanja odvija se za nekoliko mikrosekundi, a kombinovani koraci za operacije čitanja ili upisivanja traju oko deset milisekundi, što se čini sporim, ali se podacima pristupa paralelno pa je moguća brzina pristupa od 10MBps [77].

6.3.4. Metodi uništavanja medija

Destrukcija čvrstih diskova i memorija vrši se *topljenjem, lomljenjem ili mlevenjem* po odobrenom metodu. Svi mediji za skladištenje klasifikovanih podataka i informacija moraju se fizički čuvati prema standardima i *uputstvu za zaštitu* organizacije. Gradacija stepena saniranja medija nije konačna, nego više uputstvo za rad. Generalno, najčešća podela medija je u tri kategorije: *EM*, *laserski štampači/kopir mašine* i *osetljive memorije* (npr. RAM), ali ne uključuje elemente koji ne gube podatke (npr. EEPROM). Standard preporučuje četiri nivoa saniranja (Tabela 6.1), gde **0. nivo** označava da ni jedna kategorija medija nije sanirana [2]:

Tabela 6.1. Standard stepena saniranja ključnih kategorija medija

Nivo	Stepen saniranja medija
1.	EM mediji su sanirani propisanom demagnetizacijom ili presnimavanjem. Laserski štampač/kopir nije saniran. Osetljiva memorija nije sanirana.
2.	EM mediji su propisno sanirani demagnetizacijom ili dvo – tro-strukim presnimavanjem u skladu sa procenom rizika, cenom medija ili prodaje, količinom podataka i informacija i mogućnosti popravke. Nivo deklasifikacije mora biti barem dva nivoa niži od originalne. Laserski štampač/kopir i osetljiva memorija su propisno sanirani.
3.	Svi EM mediji su uništeni. Laserski štampač/kopir je propisno saniran. Osetljiva memorija je sanirana prema propisanom metodu na osnovu procene rizika, uzimajući u obzir cenu medija ili prodaje, količinu podataka i informacija i mogućnost popravke
4.	Svi magnetni mediji, laserski štampači/kopiri i osetljive memorije uništene.

6.3.5. Kriterijumi za izbor i implementaciju fizičke zaštite

Sistem fizičke zaštite kontroliše pravo, vremenski period i uslove pristupa objektima i zgradama organizacije. Fizičke i mere zaštite okruženja su efektivne i rentabilne, a implementiraju se na bazi četiri *opšta kriterijuma za izbor* [2]:

1. *mere zaštite se zahtevaju prema zakonu* (npr. izlazna vrata za VD);
2. *beznačajni troškovi, značajna korist* (npr. objekti IKTS u restriktivnom prostoru sa vratima kroz koja se retko prolazi);
3. *zaštita IKTS sprečava fatalne proboje sistema, ali ima ozbiljne troškove* (npr. bekapovanje programa i podataka);
4. *procenjuje se da je mera IKTS zaštite rentabilna* (npr. zaštita od prekida električnog napajanja).

Dva sistema mogu imati istu pretnju (npr. prekid napajanja) i iste ranjivosti, ali i potpuno različite gubitke. Na raspolaganju je veći broj mera zaštite, različitih po ceni i performansama. Nabavka UPS jedinice zavisi od opterećenja, broja minuta rada i brzine reagovanja na prekid napajanja, a može se instalirati i neki generator za kraće prekide napajanja ili kao rezervni izvor napajanja za UPS sistem.

6.3.6. Sistemi zaštite okruženja IKTS

Savremeno rešenje sistema fizičke zaštite okruženja IKTS čini *integrisana fizička infrastruktura*, koja obuhvata sledeće komponente [74]: (1) UPS *sistem sa distribucijom,*

(2) sistem klimatizacije sa distribucijom hladnog vazduha, (3) sistem senzora za nadzor okruženja i (4) centralnu platformu za upravljanje i monitoring.

UPS sistem sa distribucijom mora biti modularan, skalabilan, visoko raspoloživ, tehnički pouzdan i upravljiv, sa standardnim dimenzijama za IKTS opremu i napajanjem, zaštićenim od KEMZ. *Sistem klimatizacije sa distribucijom hladnog vazduha* namenjen je da hladi samo objekte i mesta gde se emituje toplota, a ne prostor. Prilagođen je rekovima sa opremom, koja ima veliku gustinu disipacije toplote. Integrisan je u IKTS i ima jedinstveno upravljanje. *Sistem senzora za nadzor okruženja IKTS* kontroliše fizički pristup, temperaturu, vlažnost i strujanje vazduha, tačku kondenzacije, opasne gasove, curenje vode, pojavu dima i buku. Takođe, vrši rano upozoravanje putem e–pošte, mobilnog telefona i pejdžera. *Jedinstvena platforma za upravljanje i monitoring* uključuje pretraživač, koji analizira trendove stanja u više rekova i ima fleksibilnu grafičku prezentaciju izlaznih rezultata u različitim formama pogodnim za brzo odlučivanje i reagovanje.

6.4. KONVERGENCIJA FIZIČKE I LOGIČKE KONTROLE PRISTUPA

U većini organizacija, sistemi logičke i fizičke kontrole pristupa funkcionišu kao dve odvojene, decentralizovano upravljane celine. Logičkom kontrolom pristupa upravlja informatičko odeljenje, a fizičkom – služba fizičko-tehničkog obezbeđenja.

Servisi fizičke zaštite deluju interaktivno sa logičkim servisima u brojnim primerima, što ukazuje na potrebu *integracije kontrola fizičkog i logičkog pristupa*. Konvergenciju logičke i fizičke zaštite u integrisani *sistem za logičko-fizičku kontrolu pristup* omogućava tehnološka integracija, kao što su: kartična kontakno-beskontaktna kontrola pristupa – zgradi, liftu, restriktivnom prostoru, računaru i bazi podataka; *bluetooth* tehologija integracije video nadzora, *piko* RM i 3PZ sistema; čitač fizičkog pristupa povezan sa PPZ sistemom, koji ga deblokira u slučaju požara; nadzor i upravljanje protokom ljudi i opreme kroz fizičke objekte; upravljanje metodama pristupa, kontrole proboja i zauzetosti prostorija itd. [35].

Na bazi ove integracije uspostavljen je *koncept upravljanja identitetom*, koji se može definisati kao *skup procesa, alata i servisa koji omogućavaju bezbedan pristup velikom skupu sistema, servisa i aplikacija sistema* [35]. *Sistem za upravljanje identitetom*, primarni je gradivni blok zaštite integrisanog sistema i sadrži sledeće interaktivne elemente:

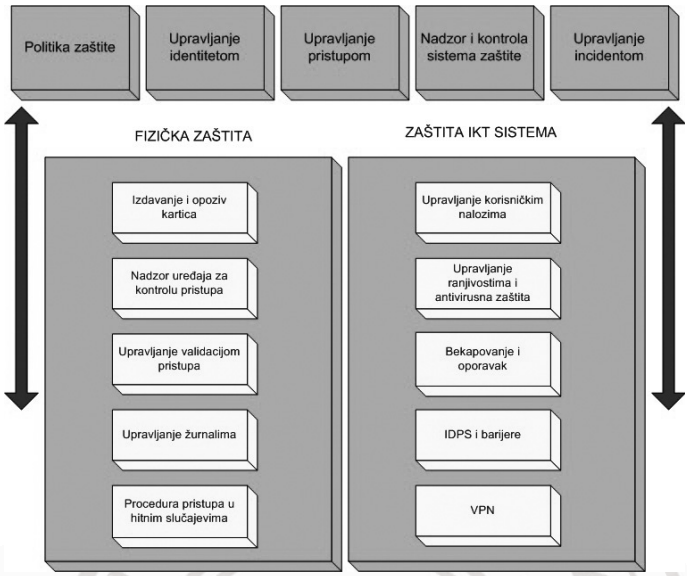
- *jedinicu za skladištenje podataka* ili logički repozitorij podataka, koji sadrži informacije iz politike zaštite i podatke o pravima pristupa korisnika;
- *jedinicu za autentifikaciju korisnika,* koja uključuje lozinku, biometrijski sistem autentifikacije ili standardne X.509 PKI sertifikate za digitalni potpis;
- *politiku zaštite,* koja definiše ko ima pristup, kojim informacijama i pod kojim uslovima i

- *jedinicu za kontrolu*, koja prati i snima tragove toka informacija, kada se podaci registruju, koriste i menjaju.

Sve ove komponente interaktivno deluju u sistemu za upravljanje identitetom i obezbeđuju: *jednokratnu identifikaciju* korisnika za primarnu autentifikaciju; *personalizaciju,* koja pridružuje neku aplikaciju ili informaciju nekom identitetu i *upravljanja pravima pristupa,* koje omogućava aplikacijama da izvrše autorizaciju na bazi informacija iz politike zaštite i datih privilegija. Konvergenciju ova dva sistema u najvećoj meri obezbeđuje PKI tehnologija i sistem *smart* kartica/tokena.

Kombinacija logičke i fizičke zaštite obezbeđuje kompletniju zaštitu od pretnji iz okruženja, sa elementima terorizma, koje zahtevaju celovit pristup problematici zaštite – od fizičke do zaštite kibernetičkog prostora. Ključni faktor konvergencije sistema fizičke i logičke kontrole pristupa postaje tehnologija, jer omogućava integraciju svih procesa u kojima može redukovati pretnje za specifične ranjivosti. Razlozi za konvergenciju ova dva sistema su brojni: *smanjenje ukupnih troškova zaštite; efikasnija kontrola pristupa i centralizovana evidencija povreda sistema zaštite; nadzor i kontrola u realnom vremenu; jedinstveni proces i lokacije za izdavanje fizičkih i logičkih identifikatora* i dr.

Da bi do ove konvergencije došlo, upravljanje integrisanim sistemom zaštitom mora integrisati postojeće procese upravljanja logičkom i fizičkom AC i personalom zaštitom IKTS organizacije. Ovakav pristup zahteva jasno definisanje vlasništva nad informacionim objektima i odgovornosti u brojnim procesima upravljanja zaštitom. Fizička zaštita podržava propisno funkcionisanje većeg broja servisa zaštite (*logičke AC, planiranja VD i kontinuiteta poslovanja i identifikacije i autentifikacije).* Kontrole fizičke zaštite obično su tesno povezane sa aktivnostima lokalne policije, stanica za PPZ**,** stanica hitne pomoći i medicinskih ustanova, koje treba konsultovati u fazi planiranja. Model odnosa fizičke i logičke AC sa procesima upravljanja sistemom zaštite organizacije prikazan je na Sl. 6.2. [35].



Sl. 6.2. Model odnosa logičke i fizičke kontrole pristupa [35]

6.5. REZIME

Fizička zaštita i zaštita okruženja IKTS treba da se zasnivaju na standardima i principima dobre prakse fizičke zaštite značajnih objekata. U većini zemalja u svetu definisani su standardi za računarsku sobu i radne stanice. Fizička zaštita lokacija IKTS obuhvata zaštitu od *prirodnih i humanih pretnji* i *sekundarnih aktivnosti*. Zaštitu okruženja IKTS, obezbeđuju tehnički i ljudski servisi kao što su električno napajanje, grejanje, hlađenje i telekomunikacije. Nestandardan rad ovih sistema može prekinuti rad servisa IKTS, dovesti do fizičkih oštećenja hardvera ili uskladištenih podataka. Mere fizičke zaštite IKTS obuhvataju osam glavnih oblasti.

Specifična fizička zaštita odlaganja ili ponovnog korišćenja (*reuse*) EM i optičkih medija obuhvata procese *saniranja* – brisanja što više podataka i informacija sa medija/opreme i *deklasifikacije* – uklanjanja ili redukcije nivoa klasifikacije medija/opreme. Saniranje ne menja automatski klasifikaciju, niti uključuje uništavanje medija/opreme. Proces obuhvata četiri nivoa (**0.** – nema saniranja, **4.** – uništavanje). Deklasifikacija se vrši na bazi procene rizika od otkrivanja preostalih podataka u medijima/opremi.

Savremeno rešenje sistema fizičke zaštite čini *integrisana fizička infrastruktura* okruženja IKTS, koja obuhvata UPS *sistem sa distribucijom, sistem klimatizacije sa distribucijom hladnog vazduha, sistem senzora za nadzor okruženja IKTS, jedinstvenu platformu za upravljanje i monitoring.* Tehnološka integracija sistema zaštite u mnogim oblastima fizičke i logičke AC, dovodi do konvergencije logičke i fizičke AC u integrisani sistem za upravljanje zaštitom, kojeg najbolje reprezentuje tehnologija *smart* kartica i proces *upravljanja identitetom*.

6.6. KLJUČNI TERMINI

Deklasifikacija medija: uklanjanje/redukcija nivoa klasifikacije medija ili opreme.

Demagnetizacija medija: smanjuje gustinu magnetnog fluksa primenom reverznog magnetnog polja i čini nečitljivim prethodno snimljene podatke.

Fizička zaštita IKTS i okruženja: zasniva se na standardima i principima dobre prakse zaštite značajnih objekata i obuhvata mere fizičko–tehničke zaštite zgrada i okruženja IKTS.

Fizički objekti: zgrade, druge građevinske strukture ili vozila u kojima su smešteni IKTS i/ili komponente računarske mreže.

Operativna lokacija: određuje se karakteristikama prirodnih i humanih pretnji i sekundarne štete od drugih faktora rizika.

Intercepcija podataka: presretanje informacija na prenosnom putu i prisluškivanje bez znanja legalnih korisnika: direktna opservacija, intercepcija podataka u prenosu i TEMPEST intercepcija elektronskih signala putem KEMZ.

Saniranje medija: proces brisanja što je moguće više podataka i informacija sa medija ili kompjuterske opreme.

TEMPEST (*Transient Elektro–Magnetic Pulse Surveillance Technology*)**:** tehnologija za EM intercepciju KEMZ signala ili (*Transient Elektro Magnetic Pulse Emanating Standard*) standard za zaštitu od KEMZ–a, koji definiše načine redukcije KEMZ signala.

Višekratno presnimavanje megnetnih medija: metod efikasnog brisanja podataka uzastopnim binarnim „1“, i „0“ i ponavljanjem ciklusa više puta.

Zaštita okruženja IKTS: obezbeđuje zaštitu tehničkih objekata, tehničkih i ljudskih servisa koji pomažu i podržavaju rad IKTS (napajanje, grejanje, hlađenje i telekomunikacije).

6.7. PITANJA ZA PONAVLJANJE

1. Fizički objekti u sistemu zaštite su:
   a. zgrade, druge fiksne građevinske strukture ili vozila u kojima su smešteni IKTS i/ili komponente RM
   b. prostorne karakteristike prirodnih pretnji (zemljotres, poplava i dr.)
   c. humane pretnje (provale, neredi, intercepcija signala, snimanje KEMZ signala
   d. sekundarna oštećenja (izlivanje toksičnih kemikalija, eksplozija, vatra, EM interferencije)
   e. servisi za podršku rada IKTS (napajanje, grejanje, hlađenje i telekomunikacije)
   f. fizički pristup
2. Operativna lokacija je određena na bazi:
   a. zgrade, druge fiksne građevinske strukture ili vozila u kojima su smešteni IKTS i/ili komponente RM
   b. prostornih karakteristika prirodnih pretnji (zemljotres, poplava i dr.)
   c. humanih pretnji (provale, neredi, intercepcija signala, snimanje KEMZ signala
   d. sekundarnih oštećenja, (izlivanje toksičnih kemikalija, eksplozija, vatra, EM interferencije)
   e. servisa za podršku rada IKTS (napajanje, grejanje, hlađenje i telekomunikacije)
   f. fizičkog pristupa
3. Okruženje IKT sistema su:
   a. zgrade, druge fiksne građevinske strukture ili vozila u kojima su smešteni IKTS i/ili komponente RM

b. prostorne karakteristike prirodnih pretnji (zemljotres, poplava i dr.)
c. humane pretnje (provale, neredi, intercepcija signala, snimanje KEMZ signala
d. sekundarna oštećenja, (izlivanje toksičnih kemikalija, eksplozija, vatra, EM interferencije)
e. servisi za podršku rada IKTS (napajanje, grejanje, hlađenje i telekomunikacije)
f. fizički pristup

4. Fizička zaštita IKTS i okruženja obezbeđuje i zaštitu zaposlenih, a težišno je usmerena na zaštitu IKTS od:
   a. prekida davanja servisa (DoS)
   b. krađe računarske opreme
   c. fizičkog oštećenja
   d. napada malicioznih programa
   e. neovlašćenog otkrivanja informacija
   f. gubitka kontrole integriteta IKTS
   g. narušavanja privatnosti legalnih korisnika
5. Mere fizičke zaštite se grupišu u sledeće glavne oblasti:
   a. barijere za fizički pristup
   b. zaštita od snežne lavine
   c. sistemi za grejanje, hlađenje i ventilacija
   d. zaštita od vlage
   e. kolaps fizičke strukture, vodovodne instalacije
   f. prisluškivanje podataka i uticaj EM smetnji
   g. mobilni ili prenosni IKTS
6. Osnovni načini prisluškivanja podataka su:
   a. intercepcija transmisije podataka
   b. bežično prisluškivanje
   c. direktno osmatranje
   d. elektromagnetska intercepcija kompromitujućeg zračenja (KEMZ)
   e. žično induktivno prisluškivanje
   f. elektromagnetska interferencija
7. Procese saniranja prenosnih medija i kompjuterske opreme je:
   a. brisanja što je moguće više podataka sa medija ili računarske opreme, koje
   b. ne uništava i ne menja automatski klasifikaciju medija/opreme
   c. uklanjanje ili redukcija nivoa klasifikacije medija/opreme na bazi procene rizika,
   d. odluke o otkrivanju preostalih podataka, procene ugovornih obaveza i eventualne prodaje, odlaganja i popravke opreme
   e. smanjenje gustine magnetnog fluksa, primenom reverznog magnetnog polja
8. Procese deklasifikacije prenosnih medija i kompjuterske opreme je:
   a. brisanje što je moguće više podataka sa medija ili računarske opreme, koje
   b. ne uništava i ne menja automatski klasifikaciju medija/opreme
   c. uklanjanje ili redukcija nivoa klasifikacije medija/opreme na bazi procene rizika, odluke o otkrivanju preostalih podataka, procene ugovornih obaveza i eventualne prodaje, odlaganja i popravke opreme
   d. smanjenje gustine magnetnog fluksa, primenom reverznog magnetnog polja
9. Proces demagnetizacije prenosnih medija i kompjuterske opreme je:
   a. brisanje što je moguće više podataka sa medija ili računarske opreme, koje
   b. ne uništava i ne menja automatski klasifikaciju medija/opreme
   c. uklanjanje ili redukcija nivoa klasifikacije medija/opreme na bazi procene rizika, odluke o otkrivanju preostalih podataka, procene ugovornih obaveza i eventualne prodaje, odlaganja i popravke opreme
   d. smanjenje gustine magnetnog fluksa, primenom reverznog magnetnog polja
10. Prvi standardni nivo saniranja medija obuhvata:
    a. svi magnetski mediji uništeni
    b. svi magnetski mediji su uništeni
    c. laserski printer/kopir je saniran prema propisanom metodu
    d. osetljiva memorija nije sanirana
    e. laserski printer/kopir nije saniran

11. Drugi standardni nivo saniranja medija obuhvata:
    a. osetljiva memorija je sanirana prema propisanom metodu
    b. magnetski mediji su sanirani propisanom demagnetizacijom ili presnimavanjem
    c. magnetski mediji su sanirani propisanom demagnetizacijom ili 2–3–strukim presnimavanjem u skladu sa procenom rizika (uzimajući u obzir cenu medija ili cenu prodaje, količinu podataka i informacija i mogućnost popravke)
    d. nivo deklasifikacije mora biti barem dva nivoa niži od originalne
12. Treći standardni nivo saniranja medija obuhvata:
    a. laserski printer/kopir nije propisno saniran
    b. osetljiva memorija je sanirana prema propisanom metodu na osnovu procene rizika, uzimajući u obzir cenu medija ili prodaje, količinu podataka i informacija i mogućnost popravke
    c. svi magnetski mediji su uništeni
    d. osetljiva memorija nije sanirana prema propisanom metodu
13. Četvrti standardni nivo saniranja medija obuhvata:
    a. magnetski mediji su sanirani propisanom demagnetizacijom ili 2–3–strukim presnimavanjem u skladu sa procenom rizika
    b. nivo deklasifikacije mora biti barem dva nivoa niži od originalne
    c. svi laserski printeri/kopiri uništeni
    d. sve osetljive memorije uništene
    e. laserski printer/kopir je saniran prema propisanom metodu
14. Opšti kriterijumi za izbora i implementaciju mera fizičke zaštite su:
    a. mere zaštite se zahtevaju prema zakonu i regulativi
    b. mere zaštite zahteva menadžer organizacije
    c. troškovi su beznačajni, ali je korist značajna
    d. troškovi su veliki, ali je korist značajna
    e. zaštita IKTS sprečava potencijalno fatalne napade, ali su troškovi veliki
    f. procenjuje se da je mera IKTS zaštite rentabilna
    g. procenjuje se da je mera IKTS zaštite nerentabilna
15. Integrisanu fizičku infrastrukturu sistema fizičke zaštite okruženja IKTS čine:
    a. UPS sistem sa distribucijom, sistem za kontrolu vlažnosti vazduha, sistem za video nadzor, centralnu platformu za upravljanje i monitoring
    b. UPS sistem sa distribucijom, sistem klimatizacije sa distribucijom hladnog vazduha, sistem senzora za nadzor okruženja, centralnu platformu za upravljanje i monitoring
    c. UPS sistem sa distribucijom, sistem klimatizacije, službu obezbeđenja, sistem senzora za kontrolu perimetra, centralnu platformu za upravljanje i monitoring
16. Konvergenciju logičke i fizičke kontrole pristupa omogućavaju sledeće tehnološke integracije:
    a. čitač fizičkog pristupa povezan sa PPZ sistemom
    b. čitač fizičkog pristupa povezan sa sistemom za video nadzor
    c. mrežna barijera sa IDPS sistemom
    d. AVP instaliran u mrežnoj kapiji
    e. nadzor i upravljanje protokom ljudi i opreme kroz fizičke objekte
    f. upravljanje pristupom, kontrola proboja perimetra i zauzetosti prostorija
17. Razlozi koji opravdavaju konvergenciju logičke i fizičke kontrole pristupa su:
    a. smanjenje ukupnih troškova zaštite i efikasnija kontrola pristupa
    b. centralizovana evidencija povreda sistema zaštite
    c. nadzor i kontrola u realnom vremenu
    d. nadzor i kontrola u *offline* režimu
    e. jedinstveni proces i lokacije za izdavanje fizičkih/logičkih identifikatora
    f. smanjenje obima rada na planiranju zaštite

7. UPRAVLJANJE PERSONALNOM ZAŠTITOM

Po završetku ovog poglavlja naučićete kako se:

- određuje značaj personalne zaštite u IS
- upravlja procesom popune radnih mesta u IS
- upravlja korisničkim nalozima
- kontroliše proces upravljanja korisničkim nalozima
- upravlja personalnom zaštitom u IS sa javnim pristupom

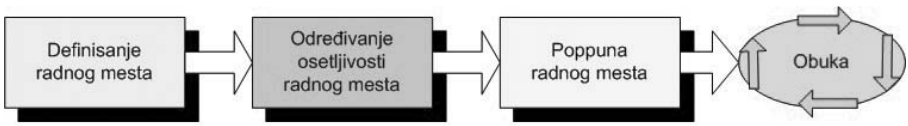
7.1. UVOD

Većina važnijih pitanja zaštite uključuje ljudski faktor – korisnike, projektante, specijaliste za implementaciju i menadžere zaštite. Širok spektar pitanja personalne zaštite odnosi se na interakciju ovih lica sa objektima informacione imovine, u procesu pristupa i autorizacije.

Personalna zaštita obuhvata i popunu kadrova za rad u IKTS i šire u organizaciji, administraciju korisnika, koji rade sa objektima sistema, uključujući zabranu pristupa zaposlenih određenim objektima IKTS, kao i administraciju pristupa javnim servisima i pristupa zaposlenih po ugovoru. Personalna zaštita usko je vezana sa servisima logičke i fizičke kontrole pristupa.

7.2. PROCES POPUNE RADNIH MESTA U IKTS

Proces popune radnih mesta u IKTS (Sl. 7.1), primenljiv na korisnike i menadžere aplikacija, menadžere IKTS i specijaliste zaštite, uključuje četiri faze: (1) d*efinisanje radnog mesta*, (2) *određivanje najvišeg nivoa osetljivosti objekata* IKTS, (3) *popunu radnih mesta* i (4) *obuku* [43].



Sl. 7.1. Proces popune zaposlenih u IKT sistemu

U fazi definisanja i opisa radnih mesta, moraju se razmatrati sva pitanja zaštite. Kada se radno mesto definiše u opštim crtama, odgovorni menadžer treba da odredi tip pristupa IKTS–u za to radno mesto. Kod određivanja prava pristupa treba primenjivati opšte principe razdvajanja dužnosti, davanje minimalnih privilegija i pristupa samo informacijama koje treba znati (engl., *need to know*) za obavljanje posla. *Razdvajanje dužnosti* odnosi se na deljenje uloga i odgovornosti, tako da ni jedan pojedinac nije nezamenljiv i da ne može sabotirati kritične procese. Definisanje radnih mesta i dužnosti zaposlenih, obaveza je menadžera. *Minimum privilegija* znači da se korisniku daje samo pristup neophodan za rad, a ne da ima ekstremno malo prava pristupa.

U opštem slučaju za smanjenje rizika, efektivnije je primenjivati principe za osetljiva radna mesta, nego bezbednosnu zaštitu zaposlenih. Primena ovih principa može ograničiti štete od slučajnog incidenta, grešaka ili neovlašćenog korišćenja IKTS. Primena minimuma privilegija ne sme uticati na zamenljivost zaposlenih na određenim radnim mestima. Kod određivanja privilegija, treba konsultovati zahteve iz plana upravljanja VD i kompjuterskim incidentom.

7.2.1. Određivanje osetljivosti radnog mesta

Za određivanje osetljivosti radnog mesta potrebno je poznavati opis radnog mesta i nivoe pristupa, koje zahteva. Odgovorni menadžeri treba da korektno identifikuju nivoe osetljivosti radnog mesta, tako da se može kompletirati odgovarajuća i rentabilna personalna zaštita. U opštem slučaju, različiti nivoi osetljivosti pripisuju se različitim radnim mestima, na bazi stepena štete, koju korisnici mogu izazvati pristupom osetljivim informacijama, procesiranim na radnom mestu. Broj osetljivih radnih mesta treba da bude racionalan, pošto zaštita većeg broja osetljivih radnih mesta zahteva više resursa, a suviše mali broj može izazvati veliki rizik [35].

7.2.2. Popuna radnih mesta i izbor zaposlenih

Faza *popune radnih mesta*, počinje sa objavljivanjem javnog konkursa u kojem se navodi, koji profil kandidata se zahteva i za koje radno mesto. Radna mesta se svrstavaju u kategorije prema osetljivosti materijala i informacija kojima se rukuje na tom radnom mestu, a menadžeri proveravaju poverljivost i pouzdanost lica za konkretno radno mesto. *Bezbednosna provera* kandidata pomaže da se odredi podobnost nekog lica za određeno radno mesto i može biti jedan od uslova za zapošljavanje. Dok se bezbednosna provera ne završi, zaposleni se ne može zvanično rasporediti na osetljivo radno mesto, niti imati pristup osetljivim informacijama i objektima IKTS.

U *javnom sektoru* bezbednosna provera tipično obuhvata proveru krivičnog dosijea u policiji, a detaljna – obuhvata radnu istoriju, obrazovanje, spisak pokretne i nepokretne imovine u vlasništvu, upotrebu zabranjenih supstanci, intervjue i razgovore sa kolegama,

prijateljima itd. Obim i intenzitet provere zavise od osetljivosti radnog mesta. Ako bezbednosna provera utvrdi kompromitaciju, ne znači da lice automatski nije podobno za neko drugo radno mesto.

U *civilnom sektoru* bezbednosna provera lica je promenljiva i neujednačena i uglavnom se svodi na proveru ličnih kvalifikacija, radnog iskustva i hobija, koje kandidati dostavljaju uz zahtev za radno mesto. Obično se novo lice postavlja na manje osetljivo radno mesto. Zaposleni u civilnom sektoru, koji rade za državnu upravu, mogu biti podvrgnuti kompletnoj bezbednosnoj proveri. Odluku treba doneti u odnosu na vrstu posla, rezultate provere i druge relevantne faktore [35].

7.2.3. Obuka zaposlenih

Popuna radnog mesta nije završena prijemom lica na neko radno mesto. Zaposleni moraju završiti pripravnički staž i obučiti se za poslove na radnom mestu, uključujući i za rad na računaru i odgovornosti u procesu zaštite. U okviru ove obuke treba promovisati svest o potrebi zaštite i opšte principe zaštite IKTS. Na bazi analize rizika, daje im se pristup samo ličnim računarima, sve dok se bezbednosna provera i obuka ne završe. Adekvatno obučeni zaposleni od presudnog su značaja za efektivno funkcionisanje IKTS i aplikacija, pa je *obuka novih korisnika kritičan faktor personalne zaštite*. Obuka i obrazovanje u zaštiti su neprekidni procesi, koji se moraju izvršavati sve dok zaposleni koriste IKTS [35].

7.3. UPRAVLJANJE KORISNIČKIM NALOZIMA

Efektivno administriranje pristupa korisnika IKTS-u bitno je za održavanje sistema zaštite i *upravljanje korisničkim nalozima,* koje obuhvata servise *identifikacije, autentifikacije i autorizacije*, *nadzora, kontrole i revizije* i *verifikacije legitimiteta naloga i ovlašćenja pristupa.*

Proces upravljanja korisničkim nalozima uključuje tri faze: (1) *podnošenje zahteva, otvaranje, izdavanje i zatvaranje korisničkih naloga, (2) praćenje korisnika i njihovih odnosnih prava za pristup i (3) upravljanje ovim funkcijama* [2].

Proces tipično počinje sa upućivanjem, menadžeru/administratoru IKTS, zahteva prvog menadžera za otvaranje korisničkog naloga zaposlenog. Za pristup nekoj aplikaciji, zahtev podnosi vlasnik aplikacije menadžeru IKTS. Zahtev sadrži nivo pristupa, kojeg treba dodeliti na osnovu radne funkcije ili specifikacije *korisničkog profila grupe* zaposlenih, koji obavljaju iste poslove. Nivo pristupa po ovom nalogu mora biti konzistentan sa zahtevom menadžera, a pridružena ovlašćenja selektivna. Za pristup aplikaciji korisnici se mogu naknadno "dodavati".

Zaposlene je potrebno informisati o njihovim nalozima. Povezivanje korisničkog imena sa položajem na radnom mestu (RBAC model LAC) može pojednostaviti administrativni rad, ali otežava reviziju i eventualnu forenzičku istragu. Povezivanja korisničkog imena sa individualnim korisnikom ima veće prednosti. Za svaki pristup moraju se uspostaviti procedure za upravljanje promenama posla (ostavka, penzionisanje i dr.). Korisno je obezbediti dodatnu obuku zaposlenih, kada dobiju svoje naloge, kao što je revizija politike za pristup objektima IKTS. Eventualno, treba zahtevati potpisivanje *Izjave o prihvatanju korisničkog naloga i pridružene lozinke* tipa: *„Ja (dole potpisani) priznajem da sam lično primio lozinke za pristup IKTS, pridružene dole navedenim korisničkim nalozima. Shvatam i prihvatam svoju odgovornost za zaštitu lozinke i obavezujem se da sprovodim sve primenljive standarde zaštite IKTS i da nikome ne otkrivam lozinke. Dalje, shvatam i prihvatam da moram izvestiti menadžera IKTS zaštite o svakom problemu kojeg uočim u korišćenju lozinke ili kada imam razloge da verujem da je poverljivost mojih lozinki kompromitovana".* Pre potpisivanja korisnika i početka perioda važnosti, sva dokumenta zaštite treba da pregleda pravnik [55].

Kada se korisnički nalozi više ne koriste, supervizor treba da obavesti menadžera aplikacija i administratora sistema, tako da se isti blagovremeno ukinu. Ovlašćenja za pristup mogu biti *trajna*, ili *privremena*. Administriranje pristupa i ovlašćenja je kontinualan proces – novi korisnički nalozi se dodaju, a stari brišu. Praćenje i ažuriranje tragova promena aplikacija nije lako, ali je važno dopustiti korisnicima pristup samo aplikacijama neophodnim za izvršavanje poslova. Takođe, treba uravnotežiti zahteve za efikasnost servisa i evidenciju relevantnih događaja, koja je neophodna za upravljanja i istragu kompjuterskog incidenta. Centralizovano upravljanje procesom korisničkog pristupa daje najbolje rezultate, ali je često decentralizovano, posebno za veće IKTS, gde se administratorima regionalnih i lokalnih RM dodeljuju ovlašćenja da kreiraju naloge i menjaju korisnička ovlašćenja ili zahtevaju neophodne promene na centralnoj lokaciji.

7.3.1. Revizija prakse upravljanja korisničkim nalozima

Praksu upravljanja korisničkim nalozima potrebno je povremeno kontrolisati na nivou aplikacija i IKTS. Treba proveravati nivoe pristupa, korišćenje privilegija, aktivnost naloga, ažurnost upravljačkih ovlašćenja, kompletnost obuke korisnika itd. Kontrolu i reviziju mogu vršiti: interni i spoljni revizori ili administratori zaštite. Dobra praksa je da menadžer aplikacija (vlasnik podataka) mesečno kontroliše sve nivoe pristupa, svih korisnika aplikacija i formalno odobrava listu pristupa. Menadžer aplikacija često jedini zna tekuće zahteve za pristupe. Nezavisni *revizor* sistema zaštite može detaljnije ispitati ovlašćenja za logički i fizički pristup.

7.3.2. Detekcija nelegalnih aktivnosti zaposlenih

Pored kontrole i revizije zaštite IKTS i analize kontrolnih tragova postoji nekoliko mehanizama za detekciju nelegalnih aktivnosti. Na primer, prevare koje zahtevaju fizičko prisustvo počinioca, mogu se otkriti na osnovu odsustva zaposlenog. Treba izbegavati stvaranje prekomerne zavisnosti od pojedinaca, posebno u državnim organizacijama i periodično obnavljati bezbednosnu proveru zaposlenih, koja može dati indikacije o mogućim ilegalnim aktivnostima i pretnjama za IKTS. Takva lica treba isključiti, kao nepouzdana za rad u IKTS.

7.3.3. Privremena zamena i interni transferi zaposlenih

Ažurno održavanje korisničkih ovlašćenja za pristup je značajan aspekt upravljanja IKTS. Korisnička ovlašćenja tipično se menjaju u slučaju privremene ili stalne *promene posla* i *otkaz sa posla* iz bilo kojeg razloga [2].

Često se od korisnika zahteva da izvršavaju poslove izvan njihovog delokruga rada, u toku odsustva drugih zaposlenih. Ovo zahteva dodatna ovlašćenja pristupa, koja se moraju izdavati propisno, pažljivo nadzirati i biti konzistentna sa principom zajedničkog obavljanja posla. Ova se ovlašćenja moraju brzo ukloniti kada više nisu potrebna. Stalne promene su neophodne kada zaposleni menjaju radno mesto u organizaciji, pa se zbog moguće zloupotrebe, obnavljaju procesi davanja ovlašćenja po nalogu i ukidanja ovlašćenja prethodnog korisnika [35].

7.3.4. Ukidanje naloga

U opštem slučaju, ukidanja naloga korisnika mogu biti *prijateljska* ili *ne–prijateljska*. Prijateljsko je kada se zaposleni dobrovoljno premešta, odbije da prihvati drugi položaj ili ode u penziju. Ne–prijateljsko ukidanje je kada se zaposleni otpušta sa posla zbog viška ili mimo njegove volje. Prva vrsta ukidanja naloga i prava pristupa mnogo je češća, ali se obe moraju razmatrati.

Prijateljsko ukidanje naloga odnosi se na regularno, uzajamno saglasno udaljavanje zaposlenog iz organizacije i primenu standardnih procedura za otpuštanje/transfer zaposlenih. Ovo zahteva blagovremeno ukidanje naloga u IKTS, potpisivanje dokumenta o otkazu, vraćanje ključeva, knjiga iz biblioteke, regulisanje drugih ne-informatičkih pitanja, kontrolu stanja dokumenata na čvrstom disku, skladištenja i bekapovanja. Zaposlenom treba dati instrukciju o čišćenju računara pre odlaska. Ako je korišćena kriptozaštita, od zaposlenog se moraju uzeti i izmeniti kriptografski ključevi, oduzeti smart kartice ili drugi autentifikacioni tokeni. Mora se razmatrati i obaveza čuvanja poverljivosti podataka i informacija i proveriti da li je zaposlenom potpuno jasno, koje podatke i informacije može,

a koje ne može otkriti na novom radnom mestu. *Ne-prijateljsko* ukidanje naloga je protiv volje i bez pristanka zaposlenog. Uključuje otkaz zbog ne-prijateljskog ponašanja zaposlenog, smanjenja radnih mesta, transfer protiv volje, otkaz zbog „*sukoba ličnosti*" ili iz bezbednosnih razloga i sl. Procedura uključuje sve aktivnosti kod dobrovoljnog otpuštanja sa posla, s tim da je neka pitanja znatno teže rešavati zbog potencijalne nesaradnje ili opstrukcije otpuštenog. Najveća pretnja od ovakve vrste otpuštanja zaposlenog dolazi od informatičara koji mogu da izmene programski kôd, modifikuju konfiguraciju sistema ili aplikacije ili na drugi način zloupotrebe IKTS. Korekcija ovih akcija može biti zahtevna, skupa i dugotrajna.

7.3.5. Personalna zaštita spoljnih saradnika po ugovoru

Saradnici pod ugovorom koji obavljaju poslove u IKTS, obično se angažuju na kraći vremenski period od regularno zaposlenih, što može uticati na rentabilnost zaštite. Angažovanje ovih lica podrazumeva odgovarajuću bezbednosnu proveru, u zavisnosti od osetljivosti mesta na koje se lice angažuje.

7.3.6. Personalna zaštita u IKTS sa javnim pristupom

U sistemima sa javnim pristupom (e-uprava, akademska mreža itd.), glavni zadatak IKTS je nesmetan, efikasan i efektivan javni pristup korisnika. U nekim slučajevima razmena podataka i informacija je interaktivna između IKTS i drugih učesnika. U opštem slučaju, kada su IKTS namenjeni za javni pristup, javljaju su dodatni bezbednosni problemi zbog *porasta pretnji, teže administracije* i *održavanja zahtevanog nivoa zaštite* informacija [55].

Generalno, može se tvrditi da su za sistem za javni pristup, faktori rizika veći, a često su veća i ograničenja za korišćenje objekata i servisa tih sistema. Pored povećanog rizika od napada spolja, IKTS sa javnim pristupom može biti predmet malicioznih aktivnosti iznutra (npr. nezadovoljni zaposleni može uneti grešku, virus i sl. u datoteke sistema) sa ciljem nanošenja štete. Napadi na sisteme sa javnim pristupom mogu imati značajan uticaj na reputaciju organizacije i poverenje klijenata/partnera/korisnika. Drugi bezbednosni problemi mogu nastati zbog nenamernih grešaka neobučenih korisnika. U IKTS koji nemaju javni pristup, postoje procedure za uključivanje korisnika u obuku, a često se zahteva i potpisivanje izjava o odgovornosti korisnika u sistemu zaštite. Pored toga, mogu se formirati profili korisnika, a sa sofisticiranim mehanizmima kontrole, mogu se otkriti neuobičajene aktivnosti korisnika. U sistemima sa javnim pristupom korisnici su obično anonimni, što značajno komplikuje administraciju zaštite [35].

7.3.7. Uspostavljanje tima za zaštitu informacija

Tim za zaštitu treba da bude sastavljen od stručnjaka i profesionalaca, motivisanih za rad u zaštiti informacija. Broj profesionalaca za zaštitu informacija u svetu se procenjuje na oko 1,66 miliona (2010.), sa tendencijom rasta na 2,7 miliona (2012.). Pokazalo se da ova profesija dobro opstaje u kriznim vremenima, sa trendom rasta zarada (*SANS Institute*, 2008.: test grupa od 2100, od njih 4,38% imali godišnju zaradu 100.000 USD i više; 75% ima diplomu inženjera i veću).

Osnovna podela rada u oblasti zaštite informacija je na – *tehničke* i *upravljačke* aktivnosti, na bazi koje se grupišu i zadaci članova tima za zaštitu (Tabela 1).

Tabela 7.1. Osnovna podela zadataka u timu za upravljanje zaštitom informacija

Tehnički	Upravljački
Računarske mreže	Politika zaštite
Sistemski programi (OS ...)	Procedure zaštite
Aplikativni programi	Uputstva zaštite

Tehnički zadaci zahtevaju komandnu liniju ili grafički korisnički interfejs, a aktivnosti zahtevaju dobro razumevanje principa zaštite i tehničke implementacije i integracije. *Upravljačke aktivnosti* u zaštiti informacija uključuju generisanje politike zaštite, što zahteva lice, koje razume poslovne procese, podršku IKTS poslovanju, bezbednosne zahteve i osnovne principe zaštite informacija. Ovi zadaci zahtevaju, uglavnom, procesor teksta. Iako su tehničke i upravljačke aktivnosti različite, potrebna je razmena informacija i međusobno razumevanje obima poslova. Na bazi osnovne podele zadataka, dele se uloge i odgovornosti u zaštiti, a u praksi zaštite, na bazi svakodnevnih aktivnosti, mogu se diferencirati sledeće proširene uloge u oblasti zaštite informacija (Tabela 7.2).

Tabela 7.2. Proširene uloge u timu za zaštitu u praksi zaštite

Tehničke uloge	Upravljačke uloge
Tester sistema zaštite (*security tester*)	Autor i pisac politike zaštite (*policy writer*)
Rukovaoc incidenta (*incident handler*)	Portparol zaštite (*security communicator*): marketing u zaštiti (svest o potrebi, obuka..) vođenje nove politike zaštite
Administrator zaštite: uređaja zaštite (IDPS, barijera, skener)	Koordinator zaštite (*security coordinator*)
Administrator zaštite: korisničkih naloga i kontrole pristupa	Rukovodilac tima za zaštitu (*security team facilitator*)
Operator nadzora sistema zaštite	Pripravnik zaštite (*security trainee*)

Tim za UR/zaštitu treba da isporuči najbolje moguće servise zaštite i ostvari najveću vrednost za poslovni sistem. Standardi najbolje prakse preporučuju da:

1. *Tim za UR* treba da:
   - obezbedi scenario, na bazi procene rizika, sa predlogom akcionog plana;
   - razumljivim jezikom upozna menadžment sa stvarnim faktorima rizika i prihvati odluku o daljem postupku;
   - evidentira sve date informacije o riziku i odluke menadžmenta;
   - skuplja informacije o poslovnim planovima i strategiji razvoja, čak i na neformalan način;
   - izvrši akcije prema planu i strategiji razvoja na što bezbedniji način i izveštava o progresu.
2. *Menadžment* treba da:
   - obezbedi potrebne ljudske, finansijske i materijalne resurse i organizacionu nezavisnost tima u radu;
   - obezbedi kriterijume, zasnovane na činjenicama, potrebne za procenu prihvatljivog rizika;
   - regularno komunicira sa *Timom za UR*;
   - koristi rezultate *Tima za UR* za razvoj strategije poslovanja i marketing, u i izvan organizacije;
   - menja onu stranu koja ne izvršava svoje obaveze i ne sledi ova uputstva.

7.4. REZIME

Personalna zaštita obuhvata popunu kadrova za rad u IKTS organizacije, administraciju korisnika koji rade sa objektima IKTS, uključujući zabranu pristupa zaposlenih određenim objektima IKTS, kao i posebnu administraciju pristupa javnim servisima i pristupa zaposlenih po ugovoru.

Proces popune radnih mesta u IKTS generalno uključuje najmanje četiri koraka i može se primeniti, na isti način, na opšte korisnike, menadžere i specijaliste zaštite: definisanje radnog mesta, određivanje najvišeg nivoa osetljivosti informacija, popunu radnih mesta i izbor i obuku zaposlenih.

Efektivno administriranje pristupa korisnika sistemu bitno je za održavanje bezbednosti IKTS. *Upravljanje korisničkim nalozima* obuhvata identifikaciju, autentifikaciju, autorizaciju, kontrolu i reviziju pristupa. Uvek postoji realna potreba kontrole i *povremene modifikacije* naloga ili *ukidanja prava pristupa* i razmatranja drugih pitanja vezanih za lica koja daju ostavke, da budu unapređena na više radno mesto, dobiju otkaz ili se penzionišu.

Uloge članova tima za zaštitu biraju se na bazi osnovne podele aktivnosti zaštite na *tehničke* i *upravljačke*, kao i na bazi prakse zaštite.

7.5. KLJUČNI TERMINI

Bezbednosna provera: utvrđivanje da li je neko lice podobno za osetljivo radno mesto.

Minimum privilegija: bezbednosni zahtev da se korisniku daje samo ona vrsta pristupa koja mu treba za obavljanje posla.

Osetljivost radnog mesta: nivo kritičnosti radnog mesta za poslovanje.

Personalna zaštita: uključuje bezbednosno pokrivanje svih učesnika u IKTS.

Razdvajanje dužnosti: deljenje uloga i odgovornosti tako da niko nije nezamenljiv.

Ukidanje naloga: može biti *prijateljsko* sa i *neprijateljsko,* bez pristanka korisnika.

Upravljanje korisničkim nalozima: podnošenje zahteva, izdavanje i zatvaranje korisničkih naloga, praćenje i upravljanje pravima za pristup korisnika.

7.6. PITANJA ZA PONAVLJANJE

1. Glavne faze u procesu popune radnih mesta u IKTS su:
   aq. definisanje, određivanje profila, popuna i obuka za radno mesto
   b. definisanje, određivanje osetljivosti i popuna radnog mesta
   c. definisanje, određivanje osetljivosti, popuna zahteva i obuka za radno mesto
   d. definisanje, određivanje osetljivosti i obuka za radno mesto
2. Sistemski princip razdvajanja dužnosti uključuje:
   a. bezbednosni zahtev koji označava da se korisnicima daju samo pristupi neophodni za obavljanje poslova
   b. odnosi se na deljenje uloga i odgovornosti tako da ni jedan pojedinac nije nezamenljiv i da ne može sabotirati kritične procese
   c. definisanje dužnosti zaposlenih na više radnih mesta
   d. označava da korisnici imaju ekstremno malo prava pristupa objektima sistema
3. Sistemski princip davanje minimuma privilegija uključuje:
   a. bezbednosni zahtev koji označava da se korisnicima daju samo pristupi neophodni za obavljanje poslova
   b. odnosi se na deljenje uloga i odgovornosti tako da ni jedan pojedinac nije nezamenljiv i da ne može sabotirati kritične procese
   c. definisanje radnih mesta i dužnosti zaposlenih
   d. označava da korisnici imaju ekstremno malo prava pristupa objektima sistema
4. Kritični faktor personalne zaštite za organizaciju uključuje:
   a. obuku zaposlenih
   b . upravljanje korisničkim zahtevima
   c. upravljanje personalnom zaštitom
   d. popunu radnih mesta
5. Proces upravljanja korisničkim nalogom obuhvata sledeće ključne faze:
   a. podnošenje zahteva, otvaranje, izdavanje i zatvaranje korisničkih naloga, praćenje korisnika i njihovih autorizacija, upravljanje ovim funkcijama
   b. podnošenje zahteva, otvaranje, izdavanje i zatvaranje korisničkih naloga,
   c. upravljanje zahtevima, otvaranje i zatvaranje naloga i praćenje autorizacija
6. Koju meru najpre treba preduzeti kada je otpušten radnik koji ima RS i pristup LAN–u?:

a. ukidanje korisničkog naloga
b. izmena korisničke lozinke i zabrana pristupa računaru
c. oduzimanje ključeva od kancelarije

7. Ukidanje korisničkih naloga u opštem slučaju se može okarakterisati kao:
   a. službeno i neslužbeno,
   b. prijateljsko i ne-prijateljsko
   c. pravedno i nepravedno
8. Angažovanje spoljnih saradnika u zaštiti IKTS:
   a. zahteva obavezno bezbednosnu proveru
   b. ne zahteva bezbednosnu proveru
   c. zahteva bezbednosnu proveru u zavisnosti od osetljivosti radnog mesta
9. Profili članova tima za upravljanje rizikom/zaštitom informacija, dele se na bazi osnovne podele rada u oblasti zaštite informacija:
   a. softvera i hardvera
   b. tehničke i upravljačke
   c. računarskog sistema i računarske mreže
   d. kontrola zaštite i politika zaštite
10. Povežite odgovarajuće tehničke i upravljačke zadatke članova tima za zaštitu:

Tehnički	Upravljački
1. Računarske mreže	a. Procedure zaštite
2. Sistemski programi (OS ...)	b. Uputstva zaštite
3. Aplikativni programi	c. Politika zaštite

11. Povežite uloge u organizaciji sa zadacima u zaštiti informacija:

Uloga	Zadaci
Tim za zaštitu/ UR	a. obezbedi scenario, na bazi procene rizika, sa predlogom akcija
	b. obezbedi čvrste kriterijume potrebne za procenu prihvatljivog rizika
	c. obezbedi potrebne resurse i organizacionu nezavisnost tima u radu
	d. koristi rezultate tima za UR za razvoj strategije poslovanja i marketing
	e. vrši akcije prema planu razvoja na što bezbedniji način i izveštava
Menadžment organizacije	f. evidentira sve date informacije o riziku i odluke menadžmenta
	g. razumljivim jezikom upozna menadžment sa rizikom i prihvati odluku
	h. da regularno komunicira sa timom za UR
	i. skuplja informacije o poslovnim planovima i strategiji razvoja
	j. stranu koja ne slede ova uputstva, treba menjati

8. UPRAVLJANJE OBUKOM I OBRAZOVANJEM U ZAŠTITI

Po završetku ovog poglavlja razumećete:

- značaj razvoja svesti o potrebi i obuke o zaštiti
- strukturu programa za razvoj svesti o potrebi zaštite
- strukturu programa obuke o zaštiti
- značaj kontinuiteta procesa obrazovanja o zaštiti
- upravljanje procesom razvoja svesti i obuke o zaštiti

8.1. UVOD

„Čujem i zaboravim, vidim i zapamtim, uradim i shvatim“ – Kineska poslovica.

Najslabijom komponentom sistema IKTS zaštite smatraju se korisnici – ljudi. Ova se komponenta zaštite može ojačati razvojem programa za *podizanje svesti o potrebi zaštite, obuku za sticanje veština i za formalno obrazovanje u oblasti zaštite*.

Samo korisnici, svesni svoje odgovornosti i dobro obučeni, mogu menjati svoje ponašanje i povećati odgovornost, koja je najznačajnija za poboljšanje zaštite. Promena stava korisnika, prvi je korak u promeni ponašanja. Tek sa poznavanjem potreba i mera zaštite, korisnici mogu istinski prihvatiti odgovornosti za svoje akcije i sprovoditi politiku zaštite. Nacionalni zakoni moraju obavezati menadžere, korisnike i operatere sistema na obaveznu edukaciju i obuku, adekvatnu ulogama i odgovornostima u zaštiti. Programi za razvoj svesti o potrebi zaštite, obuku i obrazovanje u zaštiti, višestruko su korisni za organizaciju i zahtevaju posebne metode i tehnike za implementaciju. Presudni su za uspeh programa za zaštitu u celini, jer ako zaposleni nisu dobro informisani o politici i procedurama zaštite, ne može se očekivati da rade efektivno na zaštiti informacija.

8.2. RAZVOJ SVESTI, OBUKA I OBRAZOVANJE U ZAŠTITI

Program za razvoj svesti o potrebi zaštite i obuku o zaštiti IKTS uključuje črtiri faze: *projektovanje, pripremu materijala, implementaciju i analizu i evaluaciju realizacije programa* [101]. Kvalitetan program za razvoj svesti o potrebi zaštite i obuku o zaštiti IKTS zasniva se na tri ključna faktora: (1) *politici i planu zaštite na bazi poslovnih potreba i procene rizika,* (2) *upoznavanju korisnika sa odgovornostima u zaštiti i* (3) *uspostavljanju*

procesa za monitorisanje i evaluaciju programa zaštite. Dobar model za obuku nudi standard COBIT. Ključni indikatori performansi obuke – **KPI** (*Key Performance Indicators*) mogu biti: *procenat polaznika obuke, vremenski period između identifikacije potrebe za obukom i same obuke, vrste interne i eksterne obuke, procenat obučenih korisnika o etičkim principima i praksi zaštite, broj incidenata po broju zaposlenih* itd. [75].

Za evaluaciju i merenje nivoa ostvarivanja ciljeva programa obuke, definišu se *kritični faktori uspeha* – **CSF** (*Critical Success Factors*), kao što su: *potrebni resursi*, *celovitost*, *značaj za karijeru, identifikovanje i dokumentovanje potreba, blagovremenost obuke, menadžerska podrška obuke, zahtev politike zaštite itd.*

Ljudski faktor je najbitniji u zaštiti i može naneti veću štetu od svih drugih izvora pretnji zajedno. Cilj ove komponente zaštite je da se smanje slučajne greške, prevare i neovlašćene aktivnosti nezadovoljnih zaposlenih. Po pravilu, *menadžeri treba da daju primer i određuju pravila ponašanja prema zaštiti*. Ako zaposleni znaju da menadžeri ne obraćaju pažnju na zaštitu, ni jedan program ne može biti efektivan. Zato je lidersko ponašanje od presudnog značaja.

Program obuke je kritičan za upoznavanje zaposlenih i nametanje obaveze sprovođenja politike zaštite. Ne može se očekivati da zaposleni sprovode politiku i procedure zaštite ili prihvataju sankcije, ako sa njima nisu upoznati. Obuka ukazuje da je primenjen standard *profesionalne odgovornosti* za zaštitu informacija, pa mnoge organizacije koriste formu *izjave o prihvatanju* kojom se zaposleni obavezuje da je pročitao i razumeo bezbednosne zahteve.

8.2.1. Program za razvoj svesti o potrebi zaštite

Razvoj svesti o potrebi zaštite nije u kategoriji obuke. Namenjen je za usmeravanje pažnje menadžera i zaposlenih na zaštitu, prepoznavanje bezbednosnih problema i adekvatno reagovanje. Razvoj svesti o potrebi zaštite motiviše menadžere i zaposlene da se odgovorno odnose prema zaštiti, ističe u kojoj meri i kako zaštita doprinosi produktivnosti i kakve su posledice loše zaštite. Dobro je izazivati izvestan osećaja straha navodeći drastične slučajeve štete od upada u sistem, ali i razbiti odbojnost zbog nerazumevanja zaštite [35].

Program razvoja svesti o potrebi zaštite može imati različite forme za različite grupe učesnika. Tipični *izvori materijala* su *obrazovne institucije, baze znanja na Internetu, profesionalne organizacije i proizvođači proizvoda zaštite, časopisi o zaštiti, konferencije, seminari i kursevi o zaštiti i dr.* Brojne su i raznovrsne tehnike i metode za implementaciju programa, uključujući video, multimedijalne CD prezentacije, štampu, postere, biltene, prospekte, demonstracije, razgovore i predavanja. Program se obično ugrađuje u osnovnu obuku o zaštiti i može koristiti svaki metod, koji menja stav zaposlenih prema zaštiti. Efektivan program za razvoj svesti o potrebi zaštite treba da obezbedi potpunu korisničku prihvatljivost.

8.2.2. Program obuke u zaštiti

Osnovna razlika između obuke i razvoja svesti o potrebi zaštite je što se obukom *osposobljavaju* korisnici za izvršavanje specifičnih funkcija zaštite, dok se programom za razvoj svesti o potrebi zaštite *usmerava pažnja* relevantnih učesnika na određena pitanja iz oblasti zaštite. Primer obuke je sertifikovani CISSP[33] kurs za specijaliste zaštite. Cilj obuke je da se korisnici osposobe sa *veštinama,* koje im omogućavaju da bezbedno izvršavaju aktivnosti u oblasti zaštite, uključujući *„šta"* i *„kako"* treba ili *„mogu"* nešto uraditi. Veština može biti *percepcijska, motorička, manuelna, intelektualna ili sociološka*. Priroda poslova u zaštiti obično zahteva kombinaciju ovih i uključuje kognitivne, psihosomatske i motoričke funkcije, zajedno sa odgovarajućim znanjem. Obuka može obuhvatiti više nivoa, od osnovne prakse zaštite, preko srednjeg do naprednog kursa obuke ili specijalizovanih veština i može biti specifična za jednu platformu ili dovoljno generička da obuhvati sve sisteme. Obuka je efektivnija kada je usmerena na specifičnu grupu. Polaznici mogu biti *opšti korisnici, specijalisti* i *profesionalci* [35].

Opšti korisnici se obučavaju za *osnovne* komponente dobre prakse zaštite, kao što su fizička zaštita prostora i opreme, zaštita lozinki i drugih autentifikacionih podataka, izveštavanje o povredama politike zaštite, politika zaštite, uloge i odgovornosti i druga pitanja koja se direktno odnose na poboljšavanje osnovne prakse zaštite korisnika. *Specijalizovana obuka* je detaljnija od osnovne, a polaznici se biraju prema *vrsti posla, funkcijama ili specifičnim tehnologijama i proizvodima koje koriste*. Izvršni menadžeri češće zahtevaju specijalizovanu, nego naprednu obuku, jer po pravilu ne moraju razumeti tehničke detalje o zaštiti, ali moraju znati da organizuju, usmeravaju i evaluiraju mere zaštite i da shvate potrebu prihvatanja preostalog rizika. *Profesionalna obuka* je specifičan vid obuke namenjen da svi korisnici, od početnika do profesionalaca u zaštiti, poseduju zahtevani nivo znanja i sposobnosti, neophodnih za njihove profesionalne odgovornosti u zaštiti. Za ovu obuku izdaju se odgovarajući sertifikati, a normalno uključuje teoretski i praktični rad, kroz kombinaciju multimedijalne prezentacije, predavanja i studija slučajeva.

8.2.3. Obrazovanje u zaštiti

Obrazovanje je proces, koji u jedinstvenu bazu znanja integriše sve veštine, sposobnosti i znanja iz različitih specijalnosti u oblasti zaštite; obuhvata koncepte i principe inter– i multi–disciplinarnih nauka i osposobljava profesionalce zaštite za proaktivne akcije [35]. Primer su specijalističke ili magistarske studije sa odgovarajućim diplomama. Program i *tehnike* obrazovanja u zaštiti, premašuju obim i granice istih za razvoj svesti i obuku u zaštiti (Tabela 8.1).

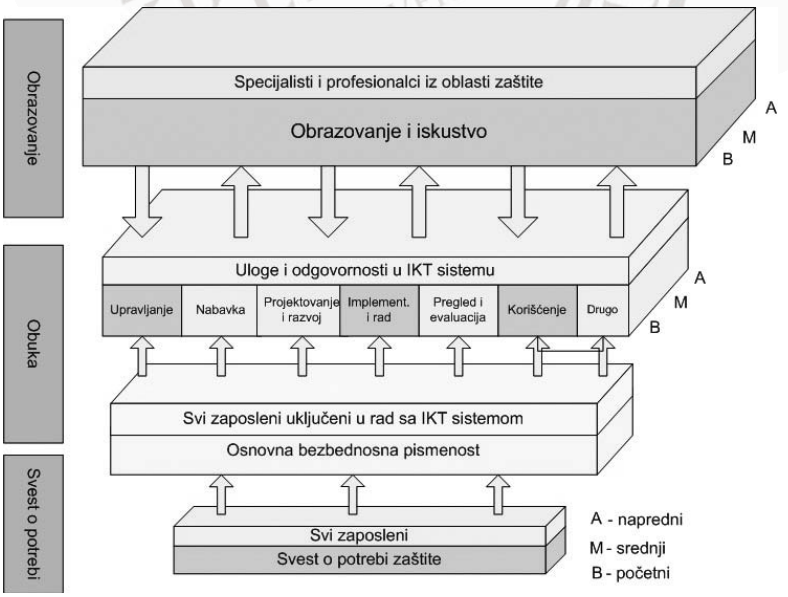
33 Engl.: CISSP - *Certified Information System Security Professional* – sertifikovani profesionalci sistema zaštite informacija.

Tabela 8.1. Komparacija parametara svesti, obuke i obrazovanja u zaštiti

PARAMETRI	SVEST O POTREBI	OBUKA	OBRAZOVANJE
Atribut	*„Šta“*	*„Kako“*	*„Zašto“*
Nivo	Informacija	Poznavanje	Detaljno znanje
Cilj	Prihvatanje potrebe	Sticanje veština	Razumevanje procesa
Metod	Multimedijska prezentacija: video, štampa, posteri	Praktična nastava: predavanja, vežbe, studije slučajeva	Teoretska nastava: seminarski, diskusije, samostalni rad
Verifikacija znanja	Tačno/pogrešno; Višestruki izbor (učenje identifikacijom)	Rešavanje problema (usvojeno znanje)	Izrada eseja (rada) (interpretacija znanja)
Vreme uticaja	Kratkoročno	Srednjeročno	Dugoročno

8.2.4. Kontinuitet procesa obrazovanja u zaštiti

Učenje i obrazovanje u zaštiti je kontinualan proces, koji počinje sa razvojem svesti o potrebi, izgrađuje se kroz obuku i kompletira u fazi obrazovanja. Model kontinuiteta procesa učenja i obrazovanja u zaštiti prikazan je na Sl. 8.1 [75, 35].



Sl. 8.1. Model kontinuiteta procesa učenja i osposobljavanja u zaštiti

Model se zasniva na premisi da je *učenje kontinualan proces*, koji počinje sa razvojem svesti o potrebi, izgrađuje se kroz obuku, a potpuno razvija kroz obrazovanje. Obezbeđuje kontekst za razumevanje i korišćenje uputstva sa metodologijom za razvoj programa obuke i pomaže da se identifikuju znanja, sposobnosti i veštine, koje zaposleni treba da poseduje na radnom mestu. Idući prema vrhu modela obuka postaje obuhvatnija i detaljnija. Svi zaposleni treba da steknu svest o potrebi zaštite. Obuka ili o*snovna bezbednosna pismenost i uloge i odgovornosti u zaštiti,* diferenciraju se na početni (***B)***, srednji (***M***) i napredni (***A***) nivo zahteva za znanjima i veštinama. Blok modela *obrazovanje i iskustvo* primenjuje se primarno na profesionalce za bezbednost i zaštitu IKTS.

8.2.5. Znanja i veštine članova tima za upravljanje zaštitom

Za optimalan rad i upravljanje sistemom zaštite, standardi najbolje prakse zaštite preporučuju skup *tehničkih* i *komunikacionih* znanja i veština, koje članovi tima za zaštitu informacija treba da poseduju (Tabela 8.2).

Tabela 8.2. Znanja i veštine članova tima za zaštitu informacija

Tehnička znanja i veštine	Komunikacione i lične osobine
Ispitivač sistema zaštite: alati za testiranje sistema zaštite (skeneri ranjivosti RS i RM), alati za testiranje sistema na proboj, programiranje, baze podataka, opšte o IKTS, GAISP principi	*Koncentracija pažnje i sklonost ka detaljima*: sposobnost usredsređene opservacije i zapažanja detalja u svakoj aktivnosti zaštite
Rukovaoc incidenta: GAISP, RM, NOSSS zaštita sistemskih i aplikativnih programa, razumevanje ispitivača i administratora zaštite, alati zaštite RS i RM, digitalna forenzika RS i RM, programiranje, pisanje	*Posvećenost dostizanju cilja*: sposobnost za kompletiranje svakog zadatka u datom vremenu
Administrator uređaja zaštite: upravljanje barijarom, osnove Unix i Windows OS, koncept RM, autentifikacioni uređaji, operativne procedure	*Prihvatanje greške*: sposobnost timske otpornosti na neuspešne akcije i aktivnosti u zaštiti
Administrator korisničkog naloga i pristupa: detaljno poznavanje Win i Unix/Linux OS, bazično razumevanje korisničkih repozitorija (*LDAP, Active Directory*), određena znanja osnovnih GAISP i izrade operativnih procedura	*Tolerantnost*: sposobnost prihvatanja mesta i uloge sistema zaštite informacija u poslovnom sistemu, konstruktivnog i miroljubivog reagovanja, bez arogancije prema bilo kome
Operator nadzora sistema zaštite: osnovno znanje uobičajenih OS i protokola RM, pisanje, operativne procedure, opšti koncept analize događaja (log datoteka) i odgovora na alarme	*Komunikativnost*: sposobnost potpune komunikacije (sa razumevanjem) sa tehničkim i netehničkim osobljem

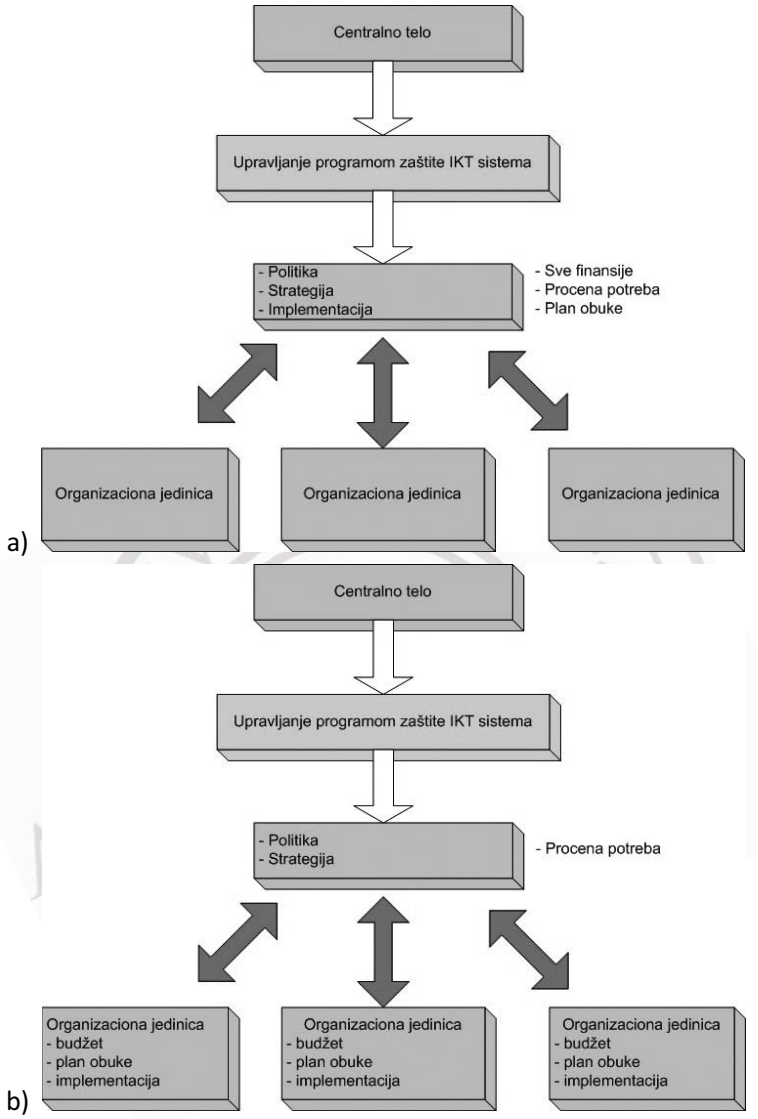
Tehnička znanja i veštine	Komunikacione i lične osobine
Kreator politike zaštite: osnovno razumevanje poslovnih procesa, analiza procesa, sinteza i skiciranje nacrta, pregovaranje, iskustvo sa tehničkom konfiguracijom IKTS i procesom revizije, ISO/IEC 27001 i COBIT standardi	*Samoorganizovanost*: sposobnost organizovanja aktivnosti u raspoloživom vremenu, resursima i prioritetima, bez potrebe za posebnim nadzorom
Koordinator zaštite: poslovna i strategija zaštite, tehnička i upravljačka iskustva, analiza poslovanja, osnovni principi IKTS i sistema zaštite za podršku poslovnih procesa	*Neprekidno učenje*: sposobnost neprekidnog praćenja i usavršavanja znanja iz oblasti zaštite (alata, promena itd.) na specijalizovanim kursevima
Pripravnik zaštite: student diplomac iz oblasti zaštite, sa poznavanjem komandne linije i GUI	*Otpornost na stres*: sposobnost rada pod pritiskom
	Kontrola strasti: sposobnost balansiranja snažnih emocija prema zaštiti i želje da se završi zadatak
	Raznovrsnost i inovacije: sposobnost posedovanja različitih znanja i veština i inovacija rešenja zaštite

Svaka ljudska akcija ima neko specifično usmerenje i nalazi se u okviru specifičnog ponašanja. *Motivacija* je interni pokretač, koji određuje to usmerenje i aktivira takvo ponašanje. U timu za upravljanje zaštitom informacija, rukovodilac tima treba da kreira okruženje, koje motiviše svakog člana tima.

8.3. UPRAVLJANJE PROGRAMOM OBUKE U ZAŠTITI

Zavisno od veličine i geografske disperzije IKTS, uloga i odgovornosti i namenjenih resursa, za upravljanje programom za obuku u zaštiti koriste se tri modela [75]: *centralizovani, delimično decentralizovani* i *decentralizovani.*

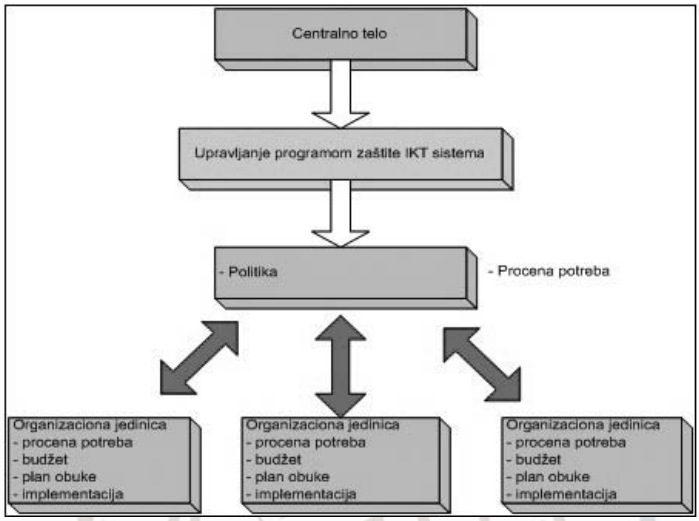
Centralizovano upravljanje primenjuje se u manjim organizacijama koje imaju slične ciljeve poslovanja u svim organizacionim jedinicama ili imaju na nivou upravljanja, neophodne resurse, ekspertizu i znanja o svim poslovima organizacionih jedinica. Odgovornost i budžet za program obuke organizacije su kod centralnog organa, koji koordinira razvoj, planiranje, realizaciju i evaluaciju programa obuke (Sl. 8.2a) [75].



Sl. 8.2. Centralizovano - (a) i delimično decentralizovano - (b) upravljanje programom obuke

Delimično decentralizovano upravljanje programom obuke u zaštiti, pogodno je za srednje i relativno veće organizacije koje imaju decentralizovanu strukturu, upravljanje i odgovornosti; imaju geografski distribuirane organizacione jedinice sa različitim misijama i ciljevima poslovanja. Politiku i strategiju razvoja programa definiše centralno telo za zaštitu, a implementaciju – izvršni menadžeri, koji raspolažu sa resursima i odgovorni su za realizaciju (Sl. 8.2b).

Decentralizovano upravljanje primenjuju relativno velike organizacije, koje imaju decentralizovanu strukturu (Sl. 8.3) sa centralizovanim opštim i distribuiranim specifičnim odgovornostima.



Sl. 8.3. Decentralizovano upravljanje programom obuke u zaštiti

Ove organizacije imaju geografski distribuirane ili poluautonomne organizacione jedinice sa različitim poslovnim ciljevima. Centralni organ zaštite distribuira politiku, zahteve i očekivanja od programa obuke, a odgovornost za realizaciju prenosi na organizacione jedinice.

8.4. PROCES RAZVOJA PROGRAMA OBUKE U ZAŠTITI

Projektni pristup razvoju programa za obuku u zaštiti, uključujući razvoj svesti o potrebi zaštite, obuhvata procese, procedure i aktivnosti kroz četiri ključne faze životnog ciklusa programa [75]: *priprema*, *planiranje*, *implementacija* i *evaluacija*.

Faza 1: U fazi *pripreme* identifikuje se odgovarajući model *za procenu potreba* i priprema razvoj programa obuke, konzistentno izabranom modelu. *Identifikacija obima i ciljeva programa* prvi je korak. Treba specifično naglasiti, da li se obuka odnosi samo na zaposlene ili i na druge korisnike IKTS. *Izbor predavača,* koji poznaju principe i tehnologije zaštite i poseduju komunikativne sposobnosti za efektivan prenos znanja i iskustava, može uključiti zaposlene specijaliste zaštite, specijaliste izvan organizacije ili specijalizovane organizacije. Takođe se zahteva *identifikacija ciljne grupe za obuku,*

jer svi zaposleni nemaju jednake potrebe za obukom. Program obuke treba prilagoditi potrebama određene grupe korisnika. Segmentacija grupa za obuku, može se izvršiti prema *nivou znanja i svesti o potrebi zaštite*, *radnim zadacima ili funkcijama*, *specifičnim kategorijama poslova*, *nivou informatičkog znanja* ili *tipu korišćene tehnologije zaštite*. *Motivacija i* razvoj svesti o potrebi zaštite, obezbeđuju podršku menadžmenta i zaposlenih. Motivacija menadžmenta je neophodna, ali nije dovoljna za uspeh programa obuke. Zaposleni moraju biti ubeđeni u korisnost zaštite, razumeti vrednosti objekata sa kojima rade i kako se zaštita odnosi na njihove poslove, što se bez odgovarajuće obuke ne može postići.

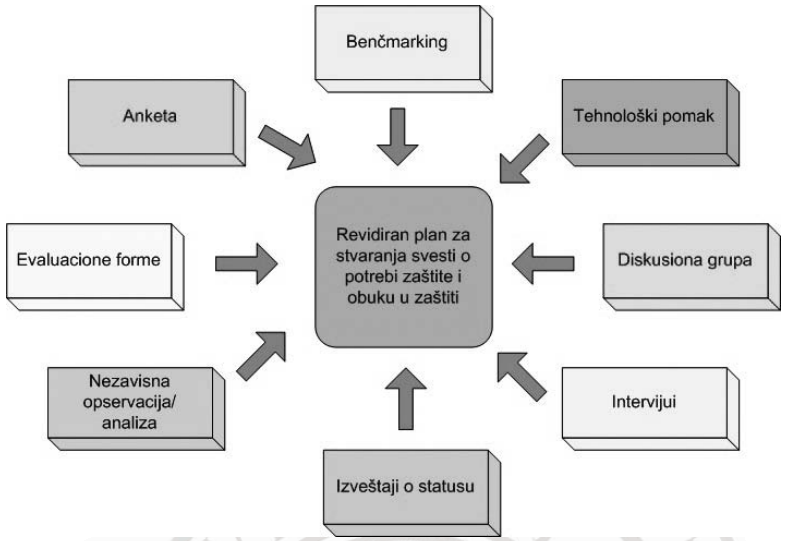
Faza 2: *Razvoj plana obuke* ubrzava pripremu i realizaciju programa obuke. Metodologija opisana u literaturi [43], obezbeđuje izradu plana i dobru pripremu materijala za brojne tipove obuke u oblasti zaštite i opisuje načine korišćenja metodologije. Za definisanje programa obuke, izbor i pripremu materijala treba koristiti pomoć specijalista za zaštitu.

Faza 3: U fazi implementacije značajne aktivnosti su *izbor tema, pronalaženje izvora i materijala za obuku i realizacija programa*. *Administracija programa* obuke o zaštiti obuhvata nekoliko važnih komponenti. *Transparentnost* je ključna za uspešnu realizaciju, ne treba obećavati ono što se ne može ispuniti. *Metodi obuke* treba da su konzistentni sa materijom koja se izlaže i prilagođeni nivou grupe. *Teme* se biraju prema potrebama korisnika. *Materijal* treba da bude što kvalitetniji, a vreme i način *prezentacije* pažljivo izabrani. U realizaciji *programa* prate se i ažuriraju sve promene tehnologija IKTS i zaštite, zakonske regulative ili politika zaštite. Program obuke mora biti aktuelan i da sadrži tekuće informacije.

Faza 4: *Rezultati evaluacije efektivnosti programa obuke* koriste se za *upravljanje promenama* – ažuriranje, korekciju i poboljšanje programa za novi ciklus obuke. Često je teško meriti efektivnost programa obuke, ali se evaluacija mora izvršiti, da se utvrdi u kojoj meri polaznici obuke usvajaju znanja i veštine. Neki metodi evaluacije koji se mogu koristiti i kombinovano su *klasična provera znanja, stepen sprovođenja procedura zaštite, korišćenje zapažanja polaznika kursa o efektima obuke i monitorisanje broja i tipova kompjuterskih incidenata pre i posle obuke.*

Proces razvoja svesti o potrebi i obuke u zaštiti treba integrisati u opštu poslovnu strategiju. Zreo program treba da definiše metriku za evaluaciju (kvalitativnu, kvantitativnu, binarnu) [75]**.** Ova komponenta zaštite odnosi se na sve ostale, a posebno na *politiku zaštite, upravljanje programom zaštite i personalnu zaštitu*.

Na Sl. 8.4. prikazani su metodi evaluacije i tehnike za ažuriranje programa obuke.



Sl. 8.4. Evaluacija i tehnike povratne sprege za kontrolu programa

8.5. REZIME

Program za razvoj svesti o potrebi i obuku u zaštiti, realizuje se kroz *projektovanje, razvoj materijala, implementaciju i analiza i evaluacija programa. Ključni indikatori sprovođenja obuke (KPI)* mogu biti procenat polaznika obuke, starosna dob polaznika i biografije (*CV*), broj vrsta obuke, broj incidenata po broju zaposlenih i sl. *Kritični faktori uspeha programa (CSF),* olakšavaju evaluaciju, a mogu biti celovitost programa, finansijska podrška i resursi, karijera i dr.

Razvoj svesti o potrebi zaštite, nije obuka nego *usmeravanje pažnje* na zaštitu, prepoznavanje bezbednosnih problema u IKTS i adekvatno reagovanje na njih. *Obuka* u zaštiti *osposobljava* zaposlene sa veštinama, potrebnim za bezbedniji rad. Može obuhvatiti više nivoa, od osnovne prakse zaštite do naprednog kursa obuke i specijalizovanih veština. *Obrazovanje u zaštiti* je proces koji integriše sva znanja i veštine iz različitih specijalnosti u jedinstvenu bazu znanja o konceptima i multidisciplinarnim principima zaštite i osposobljava specijaliste i profesionalce zaštite za proaktivnu zaštitu. *Učenje i sticanje znanja o zaštiti je kontinualan proces*, koji počinje sa razvojem svesti o potrebi, izgrađuje se kroz obuku i kompletira u procesu obrazovanja.

Za upravljanje programom obuke koriste se tri modela: centralizovano, delimično decentralizovano **i** decentralizovano upravljanje. Proces razvoja programa obuke o zaštiti, uključujući i razvoj svesti o potrebi zaštite, izvršava se kroz četiri ključne faze: *pripremu, planiranje*, *implementaciju* i *evaluaciju programa***.**

Metodologija, za pripremu i razvoj materijala za obuku, obezbeđuje pripremu materijala za brojne tipove obuke u oblasti zaštite i opisuje način korišćenja metodologije. Brojni resursi detaljno se opisuju u *Uputstvu za obuku o zaštiti*. Metodologija je fleksibilna u pogledu definisanja broja uloga u konkretnoj organizacija, a omogućava organizaciju kurseva obuke za početni, srednji i napredni nivo. Program obuke mora da pratiti promene tehnologija IKTS i zaštite, okruženja i normativnog okvira i treba ga integrisati u opštu poslovnu strategiju. Zreo proces programa obuke o zaštiti treba da definiše metriku za evaluaciju.

8.6. KLJUČNI TERMINI

Kontinuitet učenja: kontinualan proces, koji počinje sa razvojem svesti o potrebi, izgrađuje se kroz obuku i kompletira u fazi obrazovanja.

Obrazovanje u zaštiti: proces koji integriše sve veštine i znanja u oblasti zaštite različitih specijalnosti u jedinstvenu bazu znanja; obuhvata koncepte i principe multidisciplinarnih nauka i osposobljava profesionalce zaštite za proaktivnu zaštitu.

Obuka u zaštiti: osposobljava korisnike sa veštinama za bezbedno izvršavanje aktivnosti u oblasti zaštite, uključujući *„šta"* i *„kako"* treba ili *„mogu"* nešto da urade.

Program obuke: struktuiran pristup razvoju i postizanju kompetentnosti određene grupe korisnika za postizanje zahteva postavljenih u paketu obuke.

Razvoj svesti o potrebi zaštite: usmeravanje pažnje menadžera i zaposlenih na zaštitu, prepoznavanje bezbednosnih problema i reagovanje.

Sposobnost: predispozicije za određene aktivnosti; potencijalna veština.

Standard obuke: precizna izjava o zahtevanom nivou sticanja znanja, veština i sposobnosti u procesu obuke, koje se smatraju kompetentnim za izvršavanje određenog posla.

Veština: može biti percepcijska, motorička, manuelna, intelektualna ili sociološka; obično se zahteva kombinaciju ovih i uključuje kognitivne, psihosomatske i motoričke funkcije, zajedno sa odgovarajućim znanjem.

8.7. PITANJA ZA PONAVLJANJE

1. Cilj obrazovanja i obuke u zaštiti je:
   a. da se smanje slučajne greške, prevare i neovlašćene aktivnosti nezadovoljnih zaposlenih
   b. da se smanje napadi sa Interneta i socijalni inženjering
   c. . da se smanje finansijski i drugi gubici u organizaciji
   d. da se smanji odliv stručnih kadrova i drugih zaposlenih
2. Glavne faze životnog ciklusa programa za razvoj svesti i obuku u zaštiti IKTS su:
   a. Identifikacija obima i ciljeva
   b. priprema za razvoj programa
   c. projektovanje programa
   d. razvoj programa
   e. implementacija programa
   f. evaluacija programa
3. Kritični faktori za uspeh programa (CSF) za razvoj svesti i obuku u zaštiti su:
   a. podrška menadžmenta
   b. celovitost programa
   c. identifikovane i dokumentovane ranjivosti sistema
   d. finansijska podrška i resursi
   e. zahtev standarda zaštite
   f. značaj za karijeru zaposlenih
4. Sledeća faza programa obrazovanja i obuke u zaštiti je uglavnom marketinška:
   a. obuka zaposlenih za rad sa novim sistemom/komponentom zaštite
   b. obrazovanje u zaštiti za sticanje profesionalnih znanja
   c. razvoj svesti o potrebi zaštite
5. Razvoj svesti o potrebi zaštite je obuka:
   a. tačno
   b. netačno
   c. može biti povremeno
6. Najveća verovatnoća da su učesnici motivisani za program zaštite postiže se u fazi:
   a. obuke
   b. razvoja svesti o potrebi zaštite
   c. obrazovanja
7. Obuka u zaštiti je najefikasnija kada je:
   a. transparentna
   b. ima dobar metod izvođenja obuke
   c. prilagođena svim grupama korisnika
   d. ima jednostavnu, usmenu prezentaciju
8. Za upravljanje bezbednosnim funkcijama programa obuke koriste se sledeći modeli:
   a. centralizovani
   b. administrativni
   c. delimično decentralizovani
   d. decentralizovani
   distribuirani
9. Metodi za evaluaciju programa obuke su:
   a. klasična provera stečenih znanja
   b. sertifikacija i akreditacija plana evaluacije
   c. praćenje sprovođenja preporučene procedure zaštite
   d. korišćenje zapažanja polaznika kursa o efektima obuke
   e. primena metoda samoevaluacije
   f. monitorisanje broja i tipova kompjuterskih incidenata pre i posle obuke

9. SERTIFIKACIJA I AKREDITACIJA SISTEMA ZAŠTITE

Po završetku ovog poglavlja razumećete:

- metodologiju procesa sertifikacije i akreditacije (C&A):
  – *uloge i odgovornosti, kategorije akreditacije, dokumentacija, ...*
- upravljanje procesom C&A:
  – *faza pred-sertifikacije, faza sertifikacije,*
  – *faza akreditacije, faza post-akreditacije*

9.1. UVOD

Sertifikacija je proces procene efektivnosti *kontrola zaštite* IKTS, koji obezbeđuje ovlašćenom menadžeru neophodne informacije za donošenje odluke o puštanju sistema u rad. Složenost sistema je glavni problem u procesu sertifikacije, jer je za kompleksniji sistem teže detaljno evaluirati sve njegove kontrole zaštite.

Akreditacija je formalna autorizacija IKTS za rad posle integracije (pod)sistema zaštite, koju daje nadležni menadžer organizacije, na bazi rezultata procesa sertifikacije. Plan zaštite je osnovni dokument, koji se zahteva na uvid u procesu akreditacije, a mogu se zahtevati politika zaštite, rezultati procene rizika i evaluacije procesa zaštite. Ova odluka se zasniva na verifikaciji implementacije planiranog skupa upravljačkih (U), operativnih (O) i tehničkih (T) kontrola zaštite. Akreditacijom menadžment ponovo potvrđuje da prihvata preostali rizik. Formalizacija procesa akreditacije smanjuje mogućnost da IKTS bude pušten u rad, bez odgovarajuće kontrole menadžmenta. Posle značajnih promena u IKTS, okruženju ili tehnologijama zaštite, treba izvršiti re–akreditaciju, a i češće, ako je povećan rizik.

9.2. ORGANIZACIJA PROCESA SERTIFIKACIJE I AKREDITACIJE

9.2.1. Uloge i odgovornosti

Da bi na najbolji način upravljala rizikom u odnosu na ciljeve i misiju, organizacija treba da definiše uloge i odgovornosti u procesu *sertifikacije i akreditacije* – **S/A**. Ključne uloge u tipičnom programu S/A su: (1) *imenovani entitet za akreditaciju* ili *akreditator*

– **DAA** (*Designated Accreditation Authority*), (2) *sertifikator* – lice koje vrši sertifikaciju i izdaje sertifikat, (3) *rukovodilac programa* ili vlasnik sistema i (4) *specijalista za zaštitu.* Da bi se povećao integritet i objektivnost akreditacione odluke, mogu se uvesti i dodatne uloge [62].

Entitet za akreditaciju (DAA), obično je stariji menadžer sa ovlašćenjem da formalno odobri rad IKTS na prihvatljivom nivou rizika. DAA preuzima odgovornost za preostali rizik i rad sistema u određenom okruženju; ima ovlašćenja da *nadgleda budžet, odobri dokumenta o bezbednosnim zahtevima, sporazume i odstupanja od politike zaštite i da zabrani ili zaustavi rad sistema ako rizik postane neprihvatljiv.* Na osnovu rezultata sertifikacije i procene rizika DAA može formalno doneti odluku da: (1) *izda punu akreditaciju*, (2) *izda privremenu akreditaciju* ili (3) *odbije akreditaciju sistema*, ako je preostali rizik neprihvatljiv. Odluka o akreditaciji dokumentuje se u *akreditacionom paketu*, koji sadrži *izjavu o akreditaciji*, *sertifikacioni paket* i *obrazloženje odluke*. Ako je više DAA uključeno, moraju postići saglasnost i to dokumentovati u akreditacionom paketu.

Sertifikator/tim je odgovoran za procenu usaglašenosti sa bezbednosnim zahtevima za identifikaciju, procenu i dokumentovanje rizika, koordinaciju sertifikacionih aktivnosti i konsolidaciju konačnog S/A paketa. Obezbeđuje ekspertizu za vođenje nezavisne *tehničke* i *ne-tehničke* evaluacije IKTS, na osnovu bezbednosnih zahteva i kontrola sistema zaštite, dokumentovanih u planu zaštite. Procenjuje moguće pretnje, određuje korektnost implementacije kontrola zaštite i nivoa preostalog rizika. Da bi se sačuvala objektivnost sertifikacinog procesa, sertifikator treba da bude nezavisan od vlasnika, korisnika i administratora zaštite.

Rukovodilac programa i vlasnik sistema predstavljaju interese korisnika IKTS tokom životnog ciklusa sistema. Rukovodilac programa je odgovoran za sistem za vreme početnog razvoja i akvizicije, a brine se o troškovima, planu i izvršavanju plana akvizicije sistema. Pošto je sistem isporučen i instaliran, podrazumeva se da je vlasnik sistema odgovoran za sistem u toku rada, održavanja i prestanka rada sistema. Rukovodilac programa i vlasnik sistema obezbeđuju: *razvoj i rad sistema prema bezbednosnim zahtevima plana zaštite; adekvatnu obuku u zaštiti; koordinaciju rada; potrebno osoblje i informacije za sertifikatora/tim; troškove sertifikacije i uvid u sertifikacioni izveštaj pre dostavljanja DAA za akreditaciju*.

Specijalista za zaštitu sistema u radu odgovoran je za *svakodnevnu bezbednost komponenti IKTS, upravljanje incidentom, svest o potrebi zaštite, obuku i obrazovanje, pomoć u razvoju politike zaštite, usaglašenost prakse i politike zaštite, identifikovanje sistema za re-sertifikaciju ili re-akreditaciju* i za *stručno rukovođenje programom zaštite,* za sistem u razvoju [35].

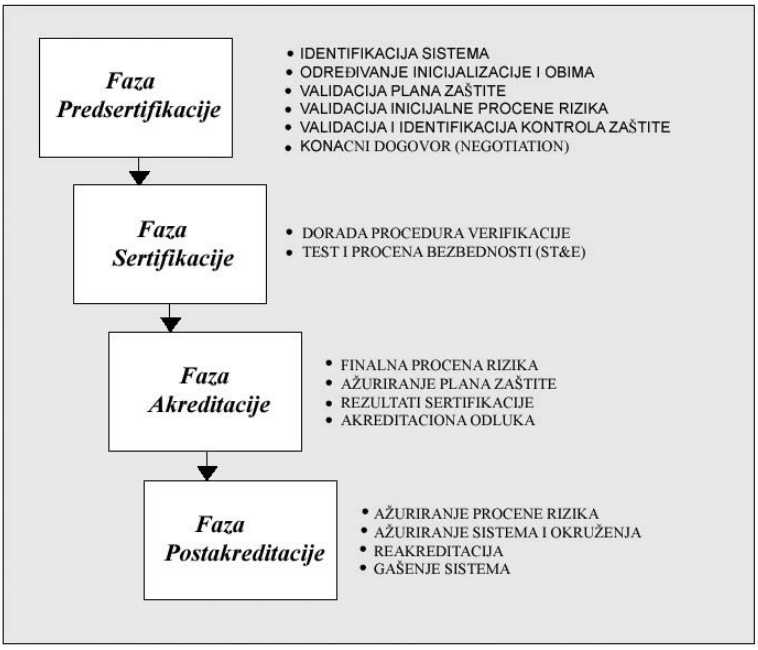
Ostale uloge i odgovornosti u procesu S/A, kao što su predstavnik korisnika, rukovodilac programa zaštite, operativni i tehnički menadžeri sistema, mogu biti uključeni u S/A proces. *Predstavnik korisnika*, koji zastupa njihove operativne interese, po potrebi pomaže u S/A procesu i učestvuje u nadzoru ispunjavanja bezbednosnih zahteva, postavljenih u planu zaštite. *Menadžer programa zaštite*, odgovoran je za primenu standardnog

S/A procesa, obezbeđuje interna uputstva i politiku za S/A proces i može da pregleda sertifikacioni paket, pre dostavljanja za akreditaciju. *Administrator zaštite* RS nadgleda operativni rad i administrira zaštitu RS. *Administrator zaštite RM* nadgleda promene i modifikacije i sprečava da se ugrozi postojeći sistem zaštite RM. Neke uloge u S/A procesu mogu biti delegirane, kao diskreciono pravo menadžera. Ulogu i odgovornost DAA ne treba delegirati izvođačima radova [35].

9.3. UPRAVLJANJE PROCESOM SERTIFIKACIJE I AKREDITACIJE

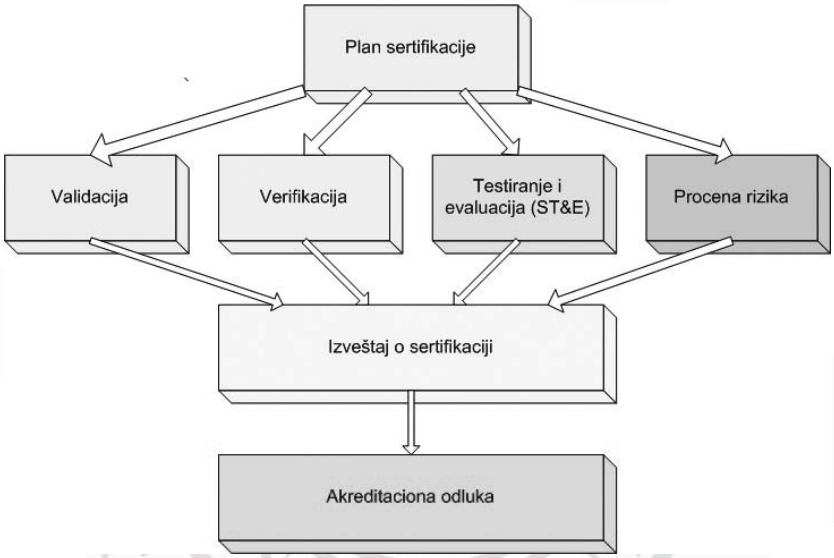
Ključne faze procesa S/A sa zadacima prikazane su na Sl. 9.1.

Faza pred–sertifikacije je pripremna i sadrži šest koraka (zadataka): *identifikacija sistema, inicijalizacija i određivanje okvira, validacija plana zaštite, validacija inicijalne procene rizika, validacija i identifikacija kontrola zaštite i konačni nalaz.* U ovoj fazi koriste se brojne informacije iz tekućeg plana zaštite, procene rizika ili druge relevantne dokumentacije zaštite. Ako plan zaštite i procena rizika nisu kompletirani, to treba uraditi pre prelaska na proces S/A. Ova faza sadrži opis svih zadataka i odgovarajućih podzadataka pred–sertifikacije [62].



Sl. 9.1. Faze i aktivnosti procesa sertifikacije i akreditacije [1]

U fazi sertifikacije kroz nezavisnu procenu, sa izabranom tehnikom i procedurom verifikacije, verifikuju se korektnost implementacije i efektivnost kontrola zaštite u praksi i usaglašenost sa bezbednosnim zahtevima. Plan faze sertifikacije (Sl. 9.2) obuhvata 4 koraka: validaciju, verifikaciju, testiranje i evaluaciju sistema zaštite – ST&E i procenu rizika. Razlike u procedurama verifikacije, između ST&E razvojnih i operativnih sistema, mogu biti u količini raspoloživih informacija [39]. Za ST&E razvojnog sistema postoje brojne pretpostavke za okruženje u kojem će sistem raditi, a koje ne mogu biti potpuno verifikovane sve dok se sistem ne pusti u rad.



Sl. 9.2. Plan sertifikacije sistema zaštite [1]

Sam *proces sertifikacije* može se izvršiti u pet koraka [62]:

1. *revizija procene rizika* (liste prioritetnih kontrola zaštite);
2. *revizija politike zaštite* (usaglašenost sa rezultatima procene rizika);
3. *revizija projektne dokumentacije* (fizički i logički dijagrami, liste itd.);
4. *revizija planova i procedura* (administracije, testiranja, revizije, plana VD) i
5. *revizija tekuće konfiguracije* (kritičnih komponenti, korišćenih alata).

Rezultati sertifikacije dokumentuju se u razvojnim ili operativnim ST&E izveštajima u sertifikacionom paketu, sa planom zaštite i konačnim izveštajem o proceni rizika u prilogu. Nakon kompletiranja faze sertifikacije, izdaje se sertifikacioni paket sa izveštajem. Kompletna lista zadataka i podzadataka u svim fazama procesa S/A, kao i skup radnih tabela za sistem merenja u fazama validacije i evaluacije u procesu sertifikacije, dati su u literaturi [62].

Postoji više *tehnika za verifikaciju* efektivnosti kontrola zaštite, koje se mogu primeniti u procesu S/A: *intervjuisanje zaposlenih u zaštiti, revizija politike, procedura i uputstava zaštite; nadzor operativnog rada i prakse zaštite; analiza testiranja sistemskog hardvera, softvera, firmware i operacija i demonstracija ponašanja sistema zaštite, obuka i vežbe*. Definisana su tri bezbednosna nivoa sertifikacije – **SLC** (*Security Level Certification*): **SLC1 –** *početni*, **SLC2 –** *srednji* i **SLC3 –** *najviši nivo* bezbednosne sertifikacija IKTS [62].

SCL1 odgovara za sve IKTS koji zahtevaju niske (N) nivoe zaštite CIA informacija, a po diskrecionom pravu i za sisteme sa S do V nivoa zaštite CIA, sa N i S rizikom. Tipično se vodi na bazi upitnika ili kontrolnih listi. Verifikuju se korektnost implementacije i efektivnost kontrola zaštite za N nivo rizika i ne zahteva se visok nivo aktivnosti. Može se izvršiti sa minimalnim resursima, intervjuisanjem, revizijom dokumentacije i posmatranjem.

SLC2 odgovara za sisteme sa S nivoom rizika, koji zahtevaju srednji nivo zaštite CIA, a po diskrecionom pravu i za sisteme sa V nivoima zaštite CIA sa N do S nivoa rizikom. Koristi sve procene iz SLC1, uz rigoroznije tehnike i procedure. Verifikuje korektnost implementacije i efektivnost kontrola zaštite IKTS za S nivo rizika i zahteva prosečan nivo aktivnosti i obim resursa. Za procenu koristi standardne, komercijalno raspoložive alate i verifikacione tehnike (intervjuisanje zaposlenih, reviziju dokumentacije i posmatranje), kao i ograničen nivo testiranja sistema zaštite (npr. funkcionalno testiranje i testiranje na proboj).

SCL3 odgovara za sisteme koji zahtevaju V nivo zaštite CIA, a koristi procene iz SLC1 i SLC2 i najrigoroznije tehnike verifikacije, koje su na raspolaganju. Verifikuje korektnost implementacije i efektivnost kontrola zaštite za V nivo rizika i zahteva visok nivo aktivnosti, značajne resurse i najsloženije alate za procenu i verifikaciju (tj. analizu sistema, prošireno funkcionalno testiranje, regresionu analizu i testiranje, demonstracije, vežbe, testiranje na proboj i dr.).

Svaki viši nivo sertifikacije dodatno povećava intenzitet i rigoroznost primene tehnika verifikacije sa prethodnog nivoa. Nivoe SLC treba detaljno opisati u *Uputstvu za akreditaciju i sertifikaciju*, koje je sastavni deo dokumentacije zaštite. U Tabeli 9.1. sumirane su različite tehnike verifikacije u odnosu na SCL na primeru verifikacije kontrola zaštite iz familije *Identifikacije i akreditacije* [62].

Tabela 9.1. Tehnike verifikacije za nivoe bezbednosne sertifikacije

SCL	TEHNIKE VERIFIKACIJE
SCL 3	◆ **Visok intenzitet,** baziran na testiranju, nezavisna procena ◆ Analiza projekta sistema, funkcionalno testiranje sa analizom pokrivenosti ◆ Regresivna analiza i regresivno testiranje i testiranje na proboj ◆ Demonstracije/vežbe za proveru korektnosti i efektivnosti kontrola zaštite ◆ SCL1 i SCL2 tehnike verifikacije (ukoliko su odgovarajuće)
SCL 2	◆ **Srednji intenzitet,** baziran na demonstraciji, nezavisna procena ◆ Funkcionalno testiranje, regresivna analiza i regresivno testiranje ◆ Testiranje na proboj (opciono) ◆ Demonstracije/vežbe za proveru korektnosti i efektivnosti kontrola zaštite ◆ SCL1 tehnike verifikacije (ukoliko su odgovarajuće)
SCL 1	◆ **Nizak intenzitet**, baziran na kontroli, nezavisni pregled zaštite ◆ Intervju personala ◆ Pregled politika zaštite, procedura, dokumenata vezanih za sistem ◆ Nadzor operativnog rada sistema i kontrola zaštite

U procesu sertifikacije važno je razumeti *odnos između nivoa sertifikacije i kontrola zaštite*. Osnovni koncept je, da se sa porastom nivoa rizika uvode dodatne kontrole zaštite, proces sertifikacije postaje strožiji i povećava se intenzitet tehnika verifikacije. Za V nivoe rizika dodaju se novi resursi za sertifikaciju i mnogo robusnije kontrole.

9.3.1. Sertifikaciona i akreditaciona dokumentacija

Cilj procesa sertifikacije je da obezbedi potrebne informacije, na osnovu kojih DAA donosi obrazloženu akreditacionu odluku za rad nekog IKTS u datom okruženju, zasnovanu na proceni rizika. Svaki zadatak i aktivnost u procesu sertifikacije, pažljivo se planira. *Sertifkacioni paket* obično sadrži *pregledan i po potrebi dopunjen plan zaštite, izveštaj ST&E razvojnog i/ili operativnog sistema, završni izveštaj o proceni rizika i izjavu sertifikatora.*

Plan zaštite ima centralnu ulogu u oblasti upravljanja rizikom, S/A procesima i u dokumentovanju zaštite IKTS. Organizacija koja ima kompletiran plan zaštite pre početka S/A procesa, može ga koristiti u pre-sertifikacionim aktivnostima, a koja nema, može uzeti potrebne informacije iz plana za pre-sertifikacione aktivnosti za određeni S/A proces. Ukoliko je plan zaštite izrađen pre procene rizika, treba ga dopuniti rezultatima procene rizika. DAA ima diskreciono pravo da u plan zaštite uključi dodatne informacije [62].

Izveštaj ST&E je osnovna komponenta S/A procesa. ST&E određuje usklađenost IKTS sa bezbednosnim zahtevima iz plana zaštite i verifikuje da li su, u planu identifikovane kontrole zaštite, korektno i efikasno primenjene.

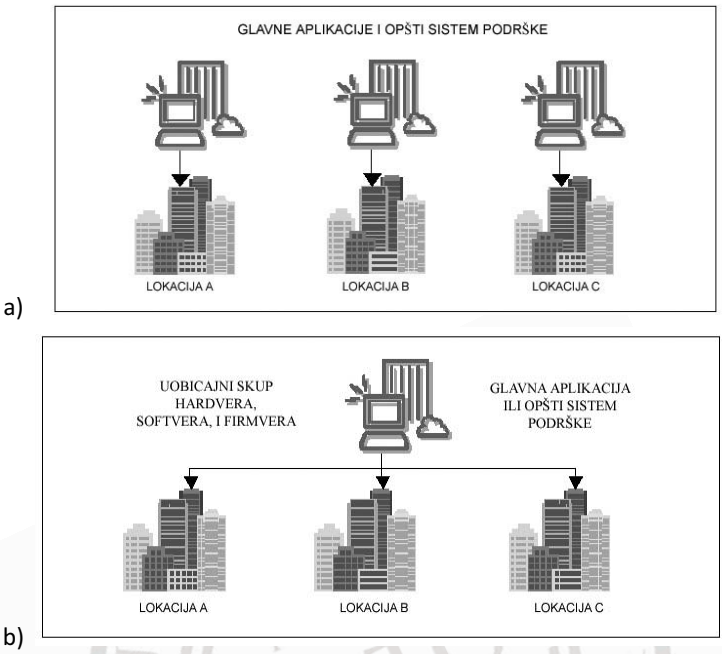
ST&E se može primeniti za sisteme u *procesu razvoja* i u *procesu rada* IKTS. Proces *ST&E sistema u razvoju* primenjuje se za nove sisteme u fazi razvoja i akvizicije ili reinženjeringa sistema. Izveštaji tipično sadrže rezultate ispitivanja i procene hardvera, softvera i *firmware*, analize arhitekture i funkcionalnog testiranja, a koriste se za verifikaciju korektnosti implementacije, efikasnosti i efektivnosti tehničkih kontrola zaštite, u skladu sa primenjenim standardima. Više se oslanja na detaljnu projektnu dokumentaciju sistema, a primenjuje se za tipske akreditacije, kao međukorak pre izvršavanja akreditacije na radnoj lokaciji. Proces *ST&E sistema u radu* primenjuje se za nove ili modifikovane sisteme, po isporuci i završetku instalacije u fazi implementacije ili na postojećim sistemima u fazi rada/održavanja. Izveštaj tipično sadrži rezultate testiranja i evaluacije lokalnog IKTS, koji se odnose na verifikaciju korektnosti implementacije, efektivnosti U, O i T kontrola zaštite i usklađenosti sa bezbednosnim zahtevima. Može da uključi i funkcionalno testiranje, testiranje na promene i analizu ranjivosti. Za reinženjering sistema u postupku S/A koriste se izveštaji ST&E sistema u razvoju i u radu.

Izveštaj o proceni rizika dokumentuje rezultate procene rizika, koji su osnova za procenu efektivnosti kontrola zaštite i donošenje odluke o prihvatljivosti preostalog rizika. Za svaki preostali rizik, obrazlažu se razlozi za prihvatanje ili odbijanje rizika, kao i za implementaciju novih kontrola zaštite za smanjenje rizika. Sertifikator procenjuje izveštaj procene rizika i određuje pouzdanost podataka. Izveštaj sertifikatora za DAA zasniva se na informacijama iz izveštaja o proceni rizika i drugim dokumentima. DAA koristi izveštaj o proceni rizika i druga dokumenta sertifikacionog paketa, da bi doneo akreditacionu odluku.

Izveštaj sertifikatora daje pregled statusa bezbednosti sistema i dovodi u vezu sve potrebne informacije za DAA, koji donosi odluku, zasnovanu na informacijama i proceni rizika. Izveštaj dokumentuje korektnost implementacije i efektivnost kontrola zaštite, kontrole koje nisu implementirane ili primenjivane i predlaže korektivne postupke.

9.3.2. Tipovi i proces akreditacije

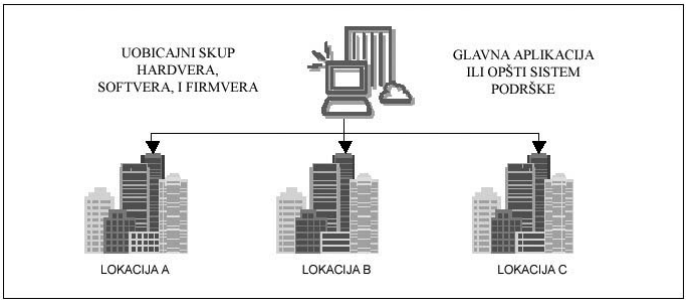
U odnosu na tip IKTS za S/A, uobičajeno se izdvajaju tri tipa procesa akreditacije: (1) *akreditacija sistema*, (2) *tipska* i (3) *lokacijska akreditacija* (Sl. 9.3a). Organizacija bira tip akreditacije, koji najviše odgovara njenim potrebama [62].



Sl. 9.3. Akreditacija sistema – (a) i tipska akreditacija – (b) [1]

Akreditacija sistema je najčešći oblik akreditacije IKTS za *glavnu aplikaciju* ili *sistem za opštu podršku,* na određenoj lokaciji, sa specifičnim ograničenjima okruženja. Sertifikacioni proces verifikuje sve bitne elemente U, O i T kontrola, a rezultat je akreditacija rada na prihvatljivom nivou preostalog rizika. *Tipska akreditacija* (Sl. 9.3b) izdaje se za IKTS za glavnu aplikaciju ili opštu podršku, koji sadrže uobičajeni skup hardvera, softvera i *firmware,* a distribuirani su na više lokacija u tipičnom radnom okruženju. DAA mora dati izjavu o preostalom riziku i jasnu definiciju radnog okruženje, identifikovati specifično korišćenje sistema, ograničenja i procedure pod kojim sistem može da radi. Značajno se smanjuje vreme trajanja procene, jer je lokalnoj organizaciji dostavljena početna dokumentacija potrebna za akreditaciju, uključujući i posebne procedure za bezbednost rada. Proces ST&E treba uraditi u centru za testiranje i integraciju ili samo na jednoj od predviđenih radnih lokacija. Instalaciju i konfiguraciju sistema zaštite treba testirati na svakoj radnoj lokaciji. Lokalno zaposleni su odgovorni za nadzor usaglašenosti radnog okruženja sa odobrenom konfiguracijom, koja je opisana u dokumentaciji o akreditaciji.

Lokacijska akreditacija (Sl. 9.4) može se izdati za sisteme za glavnu aplikaciju i/ili za opštu podršku, koji se nalaze na istoj lokaciji, u istom okruženju i sa istim faktorima rizika, a dele zajedničku strategiju i imaju uporedive ranjivosti.



Slika 9.4. Lokacijska akreditacija [1]

U fazi akreditacije dovršava se konačna procena rizika za dati IKTS, ažurira plan zaštite, sumiraju rezultati sertifikacije i donosi odluka o akreditaciji. Konačna procena rizika zasniva se na rezultatima ST&E iz faze sertifikacije. Sertifikacioni paket sadrži sve informacije, koje DAA koristi za odluku o akreditaciji. Faza akreditacije sadrži četiri koraka: *(1) konačnu procenu rizika, (2) ažuriranje plana zaštite, (3) zaključci iz faze sertifikacije i (4) donošenje odluke o akreditaciji.*

Na osnovu informacija iz sertifikacionog paketa, DAA razmatra preostali rizik za sistem i odlučuje da li da autorizuje rad sistema i prihvati preostali rizik. Kada donosi konačnu odluku, DAA može izdati: (1) *potpunu, (2) delimičnu (privremenu, uslovnu) i (3) odbijenu (ne prihvaćenu) akreditaciju* [62].

Potpuna akreditacija potvrđuje da su bezbednosni zahtevi zadovoljavajući, kontrole zaštite korektno implementirane, primenjivane i efektivno rade. Sistem je ovlašćen za rad u okruženju, navedenom u planu zaštite, sa nekoliko restrikcija u procesiranju (ako ih ima). DAA izdaje akreditaciono pismo sa dokumentacijom u prilogu, koja potvrđuje akreditacionu odluku. Ova informacija je deo finalnog *akreditacionog paketa*. Akreditaciona odluka koju daje DAA opisana je u završnom akreditacionom paketu, koji obično sadrži: (1) *akreditaciono pismo*, (2) *plan zaštite* i (3) *izveštaje,* koji dokumentuju osnovu za akreditacionu odluku. U većini slučajeva akreditacioni paket se izvodi iz sertifikacionog, a mogu se izostaviti i osetljive informacije iz plana zaštite, ST&E izveštaja i izveštaja o proceni rizika.

Delimična akreditacija potvrđuje da nema usaglašenosti sa svim bezbednosnim zahtevima iz plana zaštite i svim kontrolama zaštite – nisu primenjene ili ne rade efektivno. Potreba za sistemom je kritična, pa se pušta u rad, jer ne postoje druge mogućnosti. Da bi se smanjio povećani rizik, ova akreditacija odobrava privremeni rad sistema, u određenom periodu i pod određenim uslovima, do potpune akreditacije sistema, što se specificira u odluci DAA. Sve se restrikcije pažljivo kontrolišu, a akreditacioni akcioni plan je razvijen, tako da omogućava: *aktiviranje kapaciteta za brzi oporavak i uspostavljanje rada IKTS, delimičnu akreditaciju samo za kritične funkcije sistema, dostupnost resursa za kompletiranje akcionog plana i S/A zadataka, završetak akcionog plana u*

okviru vremena koje specificira DAA, smanjenje rizika do najnižeg mogućeg nivoa i prihvatljivost preostalog rizika.

DAA izdaje odgovarajuće akreditaciono pismo prema utvrđenim uslovima i restrikcijama i po potrebi podnosi dodatnu dokumentaciju. Tipske akreditacije mogu se smatrati delimičnim, sve dok se ne izvrši operativna ST&E, ne zadovolje odgovarajući lokalni bezbednosni zahtevi i dok se lokalne kontrole zaštite pravilno ne implementiraju i efektivno ne primenjuju. Kada se izda ova akreditacija, DAA na operativnoj lokaciji prihvata odgovornosti za bezbednost sistema i informacija.

Odbijena akreditacija potvrđuje da sistem ne odgovara bezbednosnim zahtevima i kontrolama, navedenim u planu zaštite; preostali rizik je neprihvatljivo visok, a aktivnosti sistema nisu kritične za trenutne potrebe organizacije. Sistem u razvoju nije ovlašćen za dalji razvoj, a sistem u radu se zaustavlja. DAA izdaje akreditaciono pismo o neprihvatanju rezultata sertifikacije, uključujući dodatnu dokumentaciju, koja potvrđuje odluku o odbijanju akreditacije. Primeri uzoraka teksta odluka o potpunoj, delimičnoj i odbijenoj akreditaciji i izveštaja sertifikatora dati su u literaturi [62].

Problem akreditacija velikih i kompleksnih sistema rešava se definisanjem granica i obima S/A, dekomponovanjem složenog sistema i izvršavanjem procesa S/A tih komponenti. Akreditacija složenog sistema može da sadrži jednu ili više komponenti podsistema, sertifikovanih na odgovarajućem nivou, na bazi dokumentovanog nivoa kontrola zaštite. Sertifikacioni paket je modifikovan tako da uključuje po jedan ST&E izveštaj za svaku komponentu podsistema, zajedno sa finalnim izveštajem o proceni rizika složenog sistema.

9.3.3. Faza post–akreditacije

U ovoj fazi se monitoriše status IKTS, kako bi se utvrdilo da li ima značajnih izmena u konfiguraciji sistema ili u okruženju, koje mogu imati uticaje na CIA informacija. Nadzor sistema je neophodan, da bi se održao prihvatljiv nivo preostalog rizika. Kada su promene sistema ili okruženja značajne, u odnosu na zaštitu sistema, počinju aktivnosti za re-akreditaciju. Faza postakreditacije ima tri koraka: *(1) ažuriranje procene rizika, (2) ažuriranje opisa sistema i okruženja i (3) re-akreditacija i odlaganje sistema*.

Faza post-akreditacije je kontinualan proces, kojim se ukazuje na dinamične promene tehnologije za podršku poslovnih ciljeva i misije organizacije. Uputstvo za izradu procedure za planiranje procesa S/A dato je literaturi [35].

9.4. REZIME

Sertifikacija je postupak tehničke i ne-tehničke evaluacije kontrola zaštite IKTS, koji obezbeđuje neophodne informacije za proces akreditacije, kroz kvalitativnu verifikaciju U, O i T kontrola zaštite. *Akreditacija* je proces autorizacije sistema za rad na prihvatljivom nivou rizika, posle glavne modifikacije ili razvoja novog IKTS, a obavlja je ovlašćeni entitet. Akreditacijom menadžment prihvata preostali rizik.

Metodologija razvoja procesa S/A obuhvata definisanje uloga i odgovornosti, identifikovanje IKTS za S/A, izbor tipa akreditacije, upravljanje procesom S/A i izradu S/A dokumentacije. Osnovna namena sertifikacije je definisanje korektnosti implementacije i efektivnosti kontrola zaštite. Definisana su tri bezbednosna nivoa: *nizak* (SLC1), *srednji* (SLC2) i *visok* (SLC3).

Sertifkacioni paket je konačni skup dokumenata, koje priprema *sertifikator/*tim za *akreditatora*, a obično sadrži plan zaštite, ST&E izveštaj za sistem u razvoju ili u radu, završni izveštaj o proceni rizika i izjavu sertifikatora.

Na osnovu ovih dokumenata, akreditator donosi odluku o *potpunoj, delimičnoj ili odbijenoj akreditaciji*. *Akreditacioni paket* potpune akreditacije obično sadrži akreditaciono pismo, plan zaštite i sertifikacione izveštaje, koji su osnova za akreditacionu odluku. Delimična akreditacija za osnovnu primenu sistema, privremena je potvrda za rad sistema u određenom periodu i pod određenim uslovima, do potpune akreditacije, što se specificira u odluci akreditatora. Ako sistem ne odgovara bezbednosnim zahtevima i kontrolama zaštite, navedenim u planu zaštite, preostali rizik je neprihvatljivo visok, a aktivnosti sistema nisu kritične za trenutne potrebe organizacije, akreditacioni entitet odbija akreditaciju.

Proces S/A sadrži faze: *predsertifikacije* – sadrži šest zadataka*; sertifikacije* – verifikuje korektnost implementacije i efektivnost kontrola zaštite i obuhvata procenu rizika, reviziju politike, projektne dokumentacije, plana i procedura zaštite; *akreditacije* – sadrži četiri zadatka: konačnu procenu rizika, ažuriranje plana zaštite, zaključke sertifikacije i odluku o akreditaciji *i postakreditacije* – monitoriše status datog IKTS i promena, koje mogu uticati na CIA informacija, a sadrži ažuriranje procene rizika i stanja sistema i okruženja, re-akreditaciju i odlaganje sistema.

Akreditacija velikih i kompleksnih sistema rešava se definisanjem granica procesa S/A, dekomponovanjem složenog sistema i sa S/A tih komponenti.

9.5. KLJUČNI TERMINI

Akreditacija*:* zvanična odluka menadžera da ovlašćuje rad nekog zaštićenog IKTS i da eksplicitno prihvata preostali rizik za poslove i imovinu organizacije.

Akreditacioni paket: skup dokaza za akreditatora (plan zaštite, rezultati procene rizika i sertifikacije i plan akcije), koji se koriste u procesu donošenja akreditacione odluke.

Akreditator: entitet/zvanično lice sa ovlašćenjem da formalno preuzme odgovornost za rad zaštićenog IKTS, na prihvatljivom nivou rizika za poslove i imovinu organizacije.

Glavna aplikacija*: a*plikacija koja zahteva specijalnu zaštitu zbog rizika i veličine štete od gubitka, zloupotrebe, neovlašćenog pristupa ili modifikacije informacija i aplikacije.

Granice akreditacije: sve komponente IKTS koje treba akreditovati, isključujući povezane, posebno akreditovane sisteme.

Sertifikacija*:* sveobuhvatna procena U, O i T kontrola u IKTS, koja se izvršava kao podrška procesa akreditacije i daju željene rezultate u odnosu na bezbednosne zahteve.

Sistem za opštu podršku (*General Support System)*: skup međusobno povezanih RS pod istim sistemom upravljanja, koji imaju zajedničke funkcionalnosti.

9.6. PITANJA ZA PONAVLJANJE

1. Ključne uloge u programu sertifikacije i akreditacije su:
   a. imenovani entitet za akreditaciju ili akreditator
   b. sertifikator
   c. administrator sistema
   d. rukovodilac programa ili vlasnik sistema
   e. specijalista za zaštitu
   f. administrator mreže
2. Osnovni tipovi akreditacije IKTS su:
   a. akreditacija sistema
   b. akreditacija mreže
   c. tipska akreditacija
   d. lokacijska akreditacija
   e. lokalna akreditacija
3. Procese sertifikacije je:
   a. formalna autorizacija ili odobrenje za rad IKTS i (pod)sistema zaštite.
   b. procena *kontrola zaštite* IKTS, koja obezbeđuje neophodne informacije za ovlašćenog menadžera da donese odluku za puštanje sistema u rad
   c. procena rizika i kontrola sprovođenja politike zaštite
4. Proces akreditacije je:
   a, formalna autorizacija ili odobrenje IKTS za rad posle integracije (pod)sistema zaštite
   b. procena *kontrola zaštite* IKTS koja obezbeđuje neophodne informacije za ovlašćenog menadžera da donese odluku za puštanje sistema u rad
   c. procena rizika i kontrola sprovođenja politike zaštite
5. Glavne faze procesa sertifikacije i akreditacije:
   a. faza pripreme
   b. faza pred–sertifikacije
   c. planiranje sertifikacije
   d. faza sertifikacije
   e. faza akreditacije
   f. planiranje akreditacije
   g. faza post–akreditacije

6. Revizija procene rizika u fazi sertifikacije obuhvata:
    a. formulisanje kontrole pristupa (AC), kontrole zaštite, upravljanje vanrednim događajem i upravljanja incidentom, na bazi rezultata procene rizika
    b. zadatke administracije zaštite, kontrolne zadatke testiranja proaktivne zaštite i plana vanrednih događaja
    c. kontrolu usklađenosti procena rizika sa zahtevima, što nije neophodno, jer je primarni rezultat procene rizika da obezbedi listu prioritetnih mera zaštite
    d. dokumenta koja se zahtevaju za sertifikaciju uključuju dijagrame mrežne kapije, logički dijagram i dijagram infrastrukture sistema, koncept rada, listu obaveznih i zahteva na bazi procene rizika i listu kritičnih konfiguracija
    e. proveru kritičnih komponenti konfiguracije, kojom se verifikuje da li korišćeni alati ispunjavaju zahteve i da li su iskoristivi
7. Revizija dokumentacije politike zaštite u faza sertifikacije obuhvata:
    a. formulisanje kontrole pristupa (AC), kontrole zaštite, upravljanje vanrednim događajem i upravljanja incidentom, na bazi rezultata procene rizika
    b. zadatke administracije zaštite, kontrolne zadatke testiranja proaktivne zaštite i plana vanrednih događaja
    c. kontrolu usklađenosti procena rizika sa zahtevima, što nije neophodno, jer je primarni rezultat procene rizika da obezbedi listu prioritetnih mera zaštite
    d. dokumenta koja se zahtevaju za sertifikaciju – dijagrame mrežne kapije, logički dijagram i dijagram infrastrukture sistema, koncept rada, listu obaveznih i zahteva na bazi procene rizika i listu kritičnih konfiguracija
    e. proveru kritičnih komponenti konfiguracije, kojom se verifikuje da li korišćeni alati ispunjavaju zahteve i da li su iskoristivi
8. Revizija tekuće konfiguracije u faza sertifikacije obuhvata:
    a. formulisanje kontrole pristupa (AC), kontrole zaštite, upravljanje vanrednim događajem i upravljanja incidentom, na bazi rezultata procene rizika
    b. zadatke administracije zaštite, kontrolne zadatke testiranja proaktivne zaštite i plana vanrednih događaja
    c. preporučuje se da procena rizika bude u skladu sa zahtevima, što nije neophodno. Primarni rezultat procene rizika je da obezbedi listu prioritetnih mera zaštite.
    d. dokumenta koja se zahtevaju za sertifikaciju – dijagrame mrežne kapije, logički dijagram i dijagram infrastrukture sistema, koncept rada, listu obaveznih i zahteva na bazi procene rizika i listu kritičnih konfiguracija
    e. proveru kritičnih komponenti konfiguracije, kojom se verifikuje da li korišćeni alati ispunjavaju zahteve i da li su iskoristivi
9. Revizija projektne dokumentacije u faza sertifikacije obuhvata:
    a. formulisanje kontrole pristupa (AC), kontrole zaštite, upravljanje vanrednim događajem i upravljanja incidentom, na bazi rezultata procene rizika
    b. zadatke administracije zaštite, kontrolne zadatke testiranja proaktivne zaštite i plana vanrednih događaja
    c. kontrolu usklađenosti procena rizika sa zahtevima, što nije neophodno, jer je primarni rezultat procene rizika da obezbedi listu prioritetnih mera zaštite.
    d. dokumenta koja se zahtevaju za sertifikaciju – dijagrame mrežne kapije, logički dijagram i dijagram infrastrukture sistema, koncept rada, listu obaveznih i zahteva na bazi procene rizika i listu kritičnih konfiguracija
    e. proveru kritičnih komponenti konfiguracije
10. Revizija planova i procedura u faza sertifikacije obuhvata:
    a. formulisanje kontrole pristupa (AC), kontrole zaštite, upravljanje vanrednim događajem i upravljanja incidentom, na bazi rezultata procene rizika

b. zadatke administracije zaštite, kontrolne zadatke testiranja proaktivne zaštite i plana vanrednih događaja
c. kontrolu usklađenosti procena rizika sa zahtevima, što nije neophodno, jer je primarni rezultat procene rizika da obezbedi listu prioritetnih mera zaštite
d. dokumenta koja se zahtevaju za sertifikaciju – dijagrame mrežne kapije, logički dijagram i dijagram infrastrukture sistema, koncept rada, listu obaveznih i zahteva na bazi procene rizika i listu kritičnih konfiguracija
e. proveru kritičnih komponenti konfiguracije

11. Ključni koraci faze akreditacije su:
    a. implementacija plana akreditacije
    b. konačna procena rizika
    c. tretman rizika
    d. ažuriranje plana zaštite
    e. izrada programa zaštite
    f. izvlačenje zaključaka iz faze sertifikacije
    g. donošenje odluke o akreditaciji
12. Akreditacija može biti:
    a. potpun, delimična, odbijena
    b. otvorena, zatvorena i kodirana
    c. javna, tajna i interna
13. Akreditacija sistema je:
    a. najčešći oblik akreditacije IKTS za glavnu aplikaciju ili za opštu podršku na nekoj lokaciji sa specifičnim okruženjem
    b. za IKTS za glavnu aplikaciju ili opštu podršku, koji sadrže uobičajen skup hardvera, softvera i *firmware,* a distribuirani su na više lokacija u tipičnom okruženju
    c. za IKTS za glavnu aplikaciju ili opštu podršku, koji se nalaze na istoj lokaciji, u istom okruženju i sa istim faktorima rizika i uporedivim ranjivostima
14. Tipska akreditacija je:
    a. najčešći oblik akreditacije IKTS za glavnu aplikaciju ili za opštu podršku na nekoj lokaciji sa specifičnim okruženjem
    b. za IKTS za glavnu aplikaciju ili opštu podršku, koji sadrže uobičajen skup hardvera, softvera i *firmware,* a distribuirani su na više lokacija u tipičnom okruženju
    c. za IKTS za glavnu aplikaciju ili opštu podršku, koji se nalaze na istoj lokaciji, u istom okruženju i sa istim faktorima rizika i uporedivim ranjivostima
15. Lokacijska akreditacija je:
    a. najčešći oblik akreditacije IKTS za glavnu aplikaciju ili opštu podršku na lokaciji sa specifičnim okruženjem
    b. za IKTS za glavnu aplikaciju ili opštu podršku, koji sadrže uobičajen skup hardvera, softvera i *firmware,* a distribuirani su na više lokacija u tipičnom okruženju
    c. za IKTS za glavnu aplikaciju ili opštu podršku, koji se nalaze na istoj lokaciji, u istom okruženju i sa istim faktorima rizika i uporedivim ranjivostima
16. Akreditacioni paket obično sadrži:
    a. akreditaciono pismo, plan zaštite i izveštaj
    b. akreditaciono pismo, sertifikacioni paket i izveštaj
    c. akreditaciono pismo, verifikacioni paket i izveštaj
17. Glavni zadaci faze post–akreditacije su:
    a. ažuriranje procene rizika
    b. ažuriranje plana tretman rizika
    c. ažuriranje opisa sistema i okruženja
    d. re-akreditacija i odlaganje sistema

9.7. LITERATURA

[1] American Bar Association, Section of Science &Technology Law, Privacy & Computer Crime Committee, *International Strategy for Cyberspace Security,* www.abanet.org/abapubs/books/cybercrime/, 2003.

[2] Australian Communications–Electronic Security Instruction 33, *Security Handbook*, http://www.acsi.com, 2002

[3] Bahan, C, *The Disaster Recovery Plan*, http://www.sans.org, 2003.

[4] BITS & Shared Assessments, *An Integrated Approach: ISO 27001 and BITS Shared Assessments Program*, *A Perspective of BSI Management Systems and the Shared Assessments Program,* BITS, www.bsiamerica.com, www.bitsinfo.org/fisap, 2008.

[5] BSI (Federalni IS Nemačke), *IT Baseline Protection Manual***,** *http://www.bsi.bund. de/gshb*, juli 2005.

[6] Canada, *A Guide to Business Continuity Planning*, Last modified 2/3/2005, http://www.ocipep.gc.ca/info_pro/self_help_ad/general/busi_cont_e.asp, 2005.

[7] Computer Security Incident Response Team (CSIRT), *Frequently Asked Questions (FAQ),* http://www..cert.org/csirts/csirt_faq.html, 2006.

[8] CERT Coordinating Center, *Security of the Internet, "Firewalls*," Carnegie Mellon University, SEI, http://www.cert.org/firewalls_notes/index.hatml, 2003.

[9] *CRAMM*, *www.crammusergroup.org.uk*, 2008.

[10] Domarev, V., З*ащита информации и безопасность компьютерных систем*, *http://www.security.ukrnet.net/*, 1997.

[11] Drake, D. L., Morse K. L., *The Security – Specific Eight Stage Risk Assessment Methodology*, Proceedings of the 17th National Computer Security Conference, Baltimore, Maryland, 1994.

[12] Ewell, V., C., *A methodology to the madness,* The Information Security, str 21–31, juni 2009.

[13] Ewell, V., C., *A methodology to the madness,* The Information Security, str 21–31, juni 2009.

[14] Ford, W., Baum M.S., *Secure Electronic Commerce*, Prentice Hall PTR, 2001.

[15] Freeman, W., *Business Resumption Planning: A Progressive Approach*, Version 1.2f, SANS Institute, www.sans.org, 2002.

[16] Humphrey A., *Beyond Buy–In: The Case for Executive Level Involvement in Developing a Business Continuity Plan,* GIAC Security Essentials Certification (GSEC), http://www.gsec.org, 2005.

[17] SANS Institute, *Information Security Policy & Best Practices***,** http://www.sans. org/policies, 2009.

[18] ISACA, *Standards for Information Systems Control Professionals*, http://www.isaca.org, 1999.

[19] ISACA, *IS Auditing Guideline: Application Systems Review,* Document no. 060.020.020, http://www.isaca.org, 2003.

[20] ISACA, *IS Auditing Procedure: Security Assessment Penetration Testing and Vulnerability Analysis*, Document no.8, http://www.isaca.org, 2004.

[21] ISF, *The Standard for Good Practice for Information Security*, http://www.isf.org, Ver.4, 2007.

[22] ISO/IEC 21827 (SSE CMM), *System Security Engeneering Capability Maturity Model*, http://www.iso.21827.org., 2008.

[23] ISO/IEC 27001, *Information Security Management System*, http://www.iso.27001.org, 2008.

[24] ISO/IEC 27005, **http://www. iso.27005.org**, 2008.

[25] ISO/IEC 13335, *Gudelines for the management of IT Security*, http://www.iso.13335.org, 2003.

[26] ISO/IEC 15408, *Common Criteria/ITSEC*, http://www.iso.15408.org, 2003.

[27] IT Governance Institute, *COBIT: Control Objectives for Information and related Technology,* 3rd Edition, *www.ITgovernance.org*,*www.isaca.org*, 2000.

[28] Jeffrey, R. W., Karen, M. F.*, P^3I – Protection Profile Process Improvement,* Arca Systems, Inc., william@arca.com, ferraiolo@arca.com, 2004.

[29] Kossakowski K., *DFN CERT: Bibliography of Computer Security Incident Handling Documents,* http://www.cert.dfn.de/eng/pre99papers/certbib.html, avgust 2003**.**

[30] Kissel R., Scholl M. i dr., *Guidelines for Media Sanitization*, NIST SP 800–88, 2006.

[31] Laliberte, B., *Re–architecting Disater recovery Solutions Leveraging WAN Optimization Technology*, ESG – Enterprise strategy group, white paper, 2009.

[32] Manzuik S., Pfeil K., *Network Security Assessment–from vunerability to patch, Syngress,* 2007

[33] Markus G. K., *Compromising emanations: eavesdropping risks of computer displays*, December 2003.

[34] Mehdizadeh Y. *Convergence of Logical and Physical Security,* SANS Institute, http://www.sans.org, 2004.

[35] Milosavljević M., Grubor G, *Osnovi bezbednosti i zaštite informacionih sistema*, Univerzitet Singidunum, 2006.

[36] Milosavljević M., Grubor G, *Istraga kompjuterskog kriminala - metodoloko tehnološke osnove*, Univerzitet Singidunum, 2009

[37] National Computer Security Center, *Certification and Accreditation Process Handbook for Certifiers*, NCSC–TG–031**,** Version 1, 1996.

[38] National State Auditors Association&US General Accounting Office, *Management Planning Guide for Information Systems Security Auditing*, http://www.isaca.org, 2001.

[39] Naval Research Laboratory, USA, *Handbook for the Computer Security Certification of Trusted Systems,* http://www.itd.nrl.navy.mil/ITD/5540/ publications/handbook, 1995.

[40] NIST SP 800–3, *Establishing a Computer Incident Response Capability*, http://www.nist.gov/publications, 1999.

[41] NIST SP 800–12, *An Introduction to Computer Security: The NIST Handbook*, http://www.nist.gov/publications, verzija 2004.

[42] NIST SP 800–14, *Genaerally Accepted Principles and Practices for Security*, http://www.nist.gov/publications, 2002.

[43] NIST SP 800–16, *Information Technology Security Training Requirements: A Role– and Performance–Based Model*, http://www.nist.gov/publications,1998.

[44] NIST SP 800–18, *Guide for Developing Security Plans for IT Systems,* http://www.nist.gov/publications,1998/2005.

[45] NIST SP 800–61, *Computer Security Incident Handling Guide*, http://csrc.nist.gov/ publications/nistpubs/index.html, 2004.

[46] OCTAVE®*Method Implementation Guide*, *http://www.cert.org/octave/osig.html*, 2008.

[47] Oppliger R., *Security Technologies for the World Wide Web*, Artech House, ISBN 1–58053–045–1, 2000.

[48] Orlandi, E., *The Cost of Security*, The Carnahan Conference on Security Technology, IEEE Press, New York, New York, 1991.

[49] Ozier, W., *Risk Analysis and Assessment*, Handbook of Informaton Security Management, CRC Press, Boca Raton, Florida, 1999.

[50] Pankaj, G., *CS497 – Security engineering and software engineering,* Indian Institute of technology*,* Kanpur, India, e–mail: [pankajgo]@cse.iitk.ac.in, 2005.

[51] Patrick, J., *Organizational Information Security From Scratch – A Guarantee For Doing It Right***,** SANS Institute, http://www.sans.org, 2000.

[52] Persson, E., *Digital Identity Service in Sweden,* Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2–4, 2002.

[53] Petrović, R. Slobodan, *Kompjuterski kriminal*, II Izdanje, MUP R. Srbije, 2004.

[54] Petrović, R.S., Čekerevac, Z., Grubor, G., *Security System Engineering Capability Maturity Model in The ICT Security,* 10. međunarodna naučna konferencija "Rešavanje kriznih situacija u specifičnim prostorima", Fakultet specijalnog inženjerstva, ŽU, Žilina, Slovačka, 2006.

[55] Purser, S., *A practical guide to managing information security*, Artech House, Boston, London, **http://www.artechhouse.com,** 2005**.**

[56] RealSecure, http://www.realsecure.org/security/policies, 2003.

[57] RFC 2196, *Site Security handbook,* http://www.faqs.org/rfc/rfc2196.html, 1997.

[58] RFC 792, RFC 1256, RFC 950, *http://www.icann.rfcwditor.org*, 2006.

[59] Richardson, R., *CSI 2008 Security Survey*, strana 15. http://www.gocsi.com/, 2008.

[60] Ridgway, L. E., *Disaster Recovery: Survivability & Security*. Version 1.4b GIAC Practical Assignment, 2003.

[61] Ross, R., Katzke, S., NIST SP 800–53, A, B, C, *Recommended Security Controls for Federal IS,* http://csrc.nist.gov/publications/nistpubs/800–53/sp800–53.pdf**,** 2005.

[62] Ross, R., Swanson, M., *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems,* NIST SP 800–37, http://csrc.nist. gov/publications /drafts/sp800–37–Draftver2.pdf, 2004.

[63] SANS Institute, *Information Security Policies & Best Practices***,** www.sans.org, 2009.

[64] SANS Institute, *Introduction to business continuity planning***,** www.sans.org, 2009.

[65] Savola, R., *Measurement of Security in Processes & Products*, www.vitt.ele, 2005.

[66] Schell, P.G., McLeod, Jr. R., *Management Information Systems*, 9.izdanje, Pearson Prentice Hall, SAD, 2004.

[67] Stoneburner, G., & all, *Risk Management Guide for Information Technology Systems*, SP 800–30, http://csrc.nist.gov/ publications, 2002.

[68] Stoneburner, G., Hayden, C. i Feringa, A., *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)***,** NIST SP 800–27, http://csrc.nist.gov/publications/nistpubs/800–27/sp800–27.pdf,, 2004.

[69] Tanasijević, P., *Physical Infrastructure – Base for IT Centre Security,* Tehnicom Computers, THNK Group, IDC konferencija, Beograd, 2006.

[70] UK Department of Industry, *A Taxonomic Model of Trusted Third Party Services*, Gamma Secure Systems, Diamond House, Frimley Road, Camberley, 2002.

[71] UK IT Security Evaluation & Certification Scheme Certification Body, *UK IT Security Evaluation and Certification Scheme,* www.uk.it.secscb.com, V. 3.0, 1996.

[72] US Department of Homeland Security, *Federal Computer Incident Response Center: Incident Handling Checklists,* http://www.fedcirc.gov/incident Response/IHchecklists.html, 2003.

[73] *USA CERT*, http://www.uscert.org, 2005.

[74] Velliquette, D., *Computer Security Considerations in Disaster Recovery Planning,* GIAC Security Essentials Certification (GSEC) V1.4b Option1, www.gsec.org, 2004.

[75] Wilson Mark and Hash Joan, *Building an Information Technology Security Awareness and Training Program*, NIST SP 800–50, http://www.nist.gov/publications, 2003

[76] Zadjura, J., *An Introduction to Certification and Accreditation*, SANS Institute, V. 1.4, 2003.

INTERNET IZVORI:

http://www.fas.org/irp/eprint/tempest.htm, (Pristupljeno 23.03.2010).

.http://www.phrack.org/show.php, (Pristupljeno 27.04.2010).

http://www.helpnet.securitynews.com, (Pristupljeno 21.05.2010)..

http://www. csrc.nist.gov/publications, (Pristupljeno 13.04.2010).

http://www..cert.org, 2006, (Pristupljeno 23.05.2010).

http://www.cert.org/incident_notes/index.html,(Pristupljeno 21.04.2010).

http://www.ciac.org/ciac, (Pristupljeno 23.04.2010).

http://www.fas.org/irp/eprint/tempest.htm, (Pristupljeno 3.07.2010).

http://www.first.org/team–info, (Pristupljeno 3.06.2010).

http://www.phrack.org/show.php, (Pristupljeno 7.08.2010).

http://www.sans.org/politics.html, (Pristupljeno 13.08.2010)..

www.cs.dartmouth.edu/~farid/publications/tr01.pdf, (Pristupljeno 20.08.2010).

www.isa.com, (Pristupljeno 23.07.2010).

www.isaca.com, (Pristupljeno 16.05.2010).

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

PRILOZI



UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

PRILOG 1.

ISO 27K STANDARDI – OBJAVLJENI ILI U TOKU IZRADE

- ISO/IEC 27000:2009 – provides an **overview** or introduction to the ISO27k standards and defines the specialist **vocabulary** used throughout the ISO27k series.
- ISO/IEC 27001:2005 is the **Information Security Management System (ISMS) requirements standard,** a specification for an ISMS against which thousands of organizations have been certified compliant.
- ISO/IEC 27002:2005 is the **code of practice for information security management** describing a comprehensive set of information security control objectives and a set of generally accepted good practice security controls.
- ISO/IEC 27003 will provide **implementation guidance** for ISO/IEC 27001. Due for publication in 2009.
- ISO/IEC 27004 will be an **information security management measurement** standard suggesting metrics to improve the effectiveness of an ISMS. Publication due 2009.
- ISO/IEC 27005:2008 is an **information security risk management** standard with advice on selecting appropriate risk analysis and management tools and methods.
- ISO/IEC 27006:2007 is a guide to the **certification or registration process** for accredited ISMS certification/registration bodies who award ISO/IEC 27001 certificates.
- ISO/IEC 27007 will be a guideline for **auditing Information Security Management Systems**. It is expected to focus on auditing the *management system* elements.
- ISO/IEC TR 27008 will provide **guidance on auditing information security controls**. It is expected to focus on auditing the *information security controls*.
- ISO/IEC 27010 will provide guidance on **information security management for sector–to–sector communications**.
- ISO/IEC 27011:2008 is the **information security management guideline for telecommunications organizations** (also known as ITU X.1051).
- ISO/IEC 27013 will provide guidance on the **integrated implementation of ISO/IEC 20000–1 (IT Service Management) and ISO/IEC 27001 (ISMS)**.
- ISO/IEC 27014 will cover **information security governance**.
- ISO/IEC 27015 will provide **information security management systems guidance for financial services organizations**.
- ISO/IEC 27031 will be an **ICT–focused standard on business continuity**.
- ISO/IEC 27032 will provide guidelines for **cybersecurity**.
- ISO/IEC 27033 will replace the multi–part ISO/IEC 18028 standard on **IT network security**.
- ISO/IEC 27034 will provide guidelines for **application security**.
- ISO/IEC 27035 will replace ISO TR 18044 on **security incident management**.
- ISO/IEC 27036 guideline for security of **outsourcing** (new project).
- ISO/IEC 27037 guideline for **digital evidence** (new project).

PRILOG 2.

RELEVANTNI STANDARDI ZAŠTITE

Tabela P2.1. Relevantni standardi zaštite

Standard	*Opis*
ISO 10007: 2003	*Quality management systems – Guidelines for configuration managam.*
ISO 12207: 2004	*IT – Software (sw) Life Cycle Processes*
ISO 11770–1: 1996	*IT – Security techniques – Key management – Part 1: Framework*
ISO 13335–1: 2004	*IT – Management of Information and Communications Technology Security – Part 1: Concepts and Models for ICT Security Management*
ISO 13335–2	
ISO 13888–1: 1997	*IT – Security techniques – Non–repudiation – Part 1: General*
ISO 14143–1: 1998	*IT – Software Measurement (SM) – Functional Size Measurement (FSM)*
ISO 14143–2: 2002	*IT – SM – FSM*
ISO 14143–6: 2006	*IT – Software Functional Size Measurement –FSM*
ISO/IEC 14516:2002	*IT – Security techniques – Guidelines for the use and management of TTPS*
ISO 14598–1: 1999	*IT – Software Product Evaluation – Part 1: General Overview*
ISO 14598–2: 2000	*Software Engineering – Product Evaluation – Part 2: Planning and Manag.*
ISO 14598–3: 2000	*Software Engineering – Product Evaluation – Part 3: Developer's Guide*
ISO 14598–4: 1999	*Software Engineering – Product Evaluation – Part 4: Process for Acquirers*
ISO 14598–5: 1998	*IT – Software Product Evaluation – Part 5: Process for Evaluators*
ISO 14598–6: 2001	*SE – Product Evaluation – Part 6: Documentation of Evaluation Modules*
ISO 14756: 1999	*IT – Measurement and Rating of Performance of Computer–based Sw.*
ISO 15026: 1998	*IT – System and Software Integrity Levels*
ISO 15288: 2002	*Systems Engineering (SE) – System Life Cycle Processes (SLCP)*
ISO 15408:1999	*Common Criteria (CC)*
ISO 15489–1:2001	*Information and documentation – Records management – Part 1: General*
ISO 15504–1: 2004	*IT – Process Assessment – Part 1: Concepts and Vocabulary*

Standard	*Opis*
ISO 15504–2: 2003	*IT – Process Assessment – Part 2: Performing An Assessment*
ISO 15504–3: 2004	*IT – Process Assessment – Part 3: Guidance on Performing an Assessment*
ISO 15504–4: 2004	*IT – Process Assessment – Part 4: Guidance on Use for Process Improvement and Process Capability Determination*
ISO 15504–5: 2006	*IT – Process Assessment – Part 5: An Exemplar Process Assessment Model*
ISO 15910: 1999	*IT – Software User Documentation Process*
ISO 15939: 2002	*IT – Software Measurement Process Framework*
ISO 15940: 2006	*IT – SE – Environment Services*
ISO 16085: 2004	*IT – SLCP – Risk Management*
ISO/IEC 27001	*IT – Code of Practice for Information Security Management*
ISO 18019: 2004	*Software and SE – Guidelines for the Design and Preparation of User Documentation for Application sw*
ISO 18028–1 2006	*IT – Security techniques – IT network security – Part 1: Network security management*
ISO 18028–4	*IT – Security techniques – IT Network security – Part 4: Securing remote access*
ISO 18043: 2006	*Selection, Deployment and Operations of Intrusion Detection Systems (IDS)*
ISO 19770–1: 2006	*Software Asset Management*
ISO 19796–1: 2005	*IT – Learning, Education, and Training – Quality Management, Assurance, and Metrics – Part 1: General Approach*
ISO 20000–1: 2005	*IT – Service Management – Part 1: Specification*
ISO 20000–2: 2005	*IT – Service Management – Part 2: Code of Practice*
ISO 21827 – 2007	*SSE CMM – Systems Security Engineering Capability Maturity Model*
ISO 25000: 2005	*SE – Software Product Quality Guide Requirements and Evaluation*
ISO 25051: 2006	*SE – Software Product Quality Requirements and Evaluation– Requirements for Quality of COTS Software Product and Instructions for Testing*
ISO 27001: 2005	*IT – Security Techniques – ISMS – Requirements*
ISO 9126–1: 2001	*Software Engineering – Product Quality – Part 1: Quality Model*
ISO 9796–2: 2002	*„IT – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms"*
ISO 9796–3: 2000	*2000 " IT – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms"*
ISO/AWI 14143–1: 200x	*Information Technology – Software Measurement – FSM*
ISO/DTR 25021: 200x	*Software and SE – Software Product Quality Requirements and Evaluation (SQuaRE) – Measurement Primitives*

Standard	Opis
ISO/FCD 25020: 200x	*Software and SE – Software Quality Requirements and Evaluation (SQuaRE) – Measurement Reference Model and Guide*
ISO/FCD 25030: 200x	*SE – Software Quality Requirements and Evaluation (SQuaRE)*
ISO/NP 15504–6: 200x	*IT – Process Assessment – Part 6: An Exemplar System Life Cycle Process Assessment Model*
ISO/NP 27004: 2010	*IT – Information Security Management Measurements*
ISO/NP 27005: 2000	*IT – Information Security Risk Management*
ISO/TR 13335–3: 1998	*IT – Guidelines for the Management of IT Security – Part 3: Techniques for the Management of IT Security*
ISO/TR 13335–4: 2000	*IT – Guidelines for the Management of IT Security – Part 4: Selection of Safeguards*
ISO/TR 13335–5: 2001	*IT – Guidelines for the Management of IT Security – Part 5: Management Guidance on Network Security*
ISO/TR 14143–3: 2003	*IT – Sw measurement– Functional Size Measurement (FSM)*
ISO/TR 14143–4: 2002	*IT – Software Functional Size Measurement*
ISO/TR 14143–5: 2004	*IT – Software Measurement – Functional Size Measurement (FDM)*
ISO/TR 14516: 2002	*IT – Security Techniques — Guidelines for the Use and Management of TTPS*
ISO/TR 15846: 1998	*IT – Software Life Cycle Processes: Configuration Management*
ISO/TR 16326: 1999	*SE – Guide for the Application of ISO 12207 to Project Management*
ISO/TR 18044: 2004	*Incident Management*
ISO/TR 19759: 2005	*Software Engineering – Guide to the Software Enginering Body of Knowledge*
ISO/TR 9126–2: 2003	*Software Engineering – Product Quality – Part 2: External Metrics*
ISO/TR 9126–3: 2003	*Software Engineering – Product Quality – Part 3: Quality in Use Metrics*
ISO/TR 9126–4: 2004	*Software Engineering – Product Quality – Part 4: Internal Metrics*
ISO/TR 9294: 2005	*IT – Guidelines for the Management of Software Documentation*
SP 800–12 (Oct 1995)	*An Introduction to Computer Security: The NIST Handbook.*
SP 800–18 (Dec 1998)	*Guide for Developing Security Plans for ITS guides the design and documentation of IT security controls.*
SP 800–23 (Aug 2000)	*Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*
SP 800–26 (draft r. 1)	*Security Self–Assessment Guide for Information Technology Systems*
SP 800–27 (Jun 2004 r. A)	*Engineering Principles for Information Technology Security (a baseline).*
SP 800–28 (Oct 2001)	*Guidelines on Active Content and Mobile Code.*

Standard	*Opis*
SP 800–30 (July 2002)	*Risk Management Guide for and assessment and control of IT risks.*
SP 800–34 (June 2002)	*Contingency Planning Guide for Information Technology Systems.*
SP 800–35 (Oct 2003)	*Guide to Information Technology Security Services.*
SP 800–36 (Oct 2003)	*Guide to Selecting Information Security Products.*
SP 800–37 (May 2004)	*Guide for the Security Certification and Accreditation of Federal IS.*
SP 800–40 (version 2)	*Creating a Patch and Vulnerability Management Program.*
SP 800–42 (2003)	*Guideline on Network Security Testing.*
SP 800–45 (2002)	*Guidelines on Electronic Mail Security.*
SP 800–46 (Aug 2002)	*Security for Telecommuting and Broadband Communications.*
SP 800–47 (Aug 2002)	*Security Guide for Interconnecting Information Technology Systems.*
SP 800–48 (Nov 2002)	*Wireless Network Security: 802.11, Bluetooth, and Handheld Devices.*
SP 800–50 (Oct 2003)	*Building an IT Security Awareness and Training and Education Program.*
SP 800–53 (A,B,C): 2008	*Recommended Security Controls for US Federal Information Systems.*
SP 800–55 (2003)	*Security Metrics Guide for IKTS.*
SP 800–56 (latest draft Jul 2005)	*Recommendation for Pair–Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.*
SP 800–57 Part 1 i 2 (Aug 2005)	*Recommendation on Key Management*
SP 800–58 (Jan 2005)	*Security Considerations for Voice Over IP Systems.*
SP 800–59 (Aug 2003)	*Guideline for Identifying an IS as a National Security System provides guidance on identifying an IS as a (US) national security system.*
SP 800–60 (Jun 2004)	*Guide for Mapping Types of Information and IS to Security Categories.*
SP 800–61 (Jan 2004)	*Computer Security Incident Handling Guide.*
SP 800–63 (2004)	*Electronic Authentication Guideline.*
SP 800–64 (Jun 2004)	*Security Considerations in the IS Development Life Cycle.*
SP 800–65 (Jan 2005)	*Integrating Security into the Planning and Investment Control Process.*
SP 800–70 (May 2005)	*Security Configuration Checklists Program for IT Products: comprises a set of baseline configurations for a wide variety of operating system platforms.*
SP 800–83 (Nov 2005)	*Guide to Malware Incident Prevention and Handling*
SP 800–92 (April 2006)	*Guide to Computer Security Log Management*

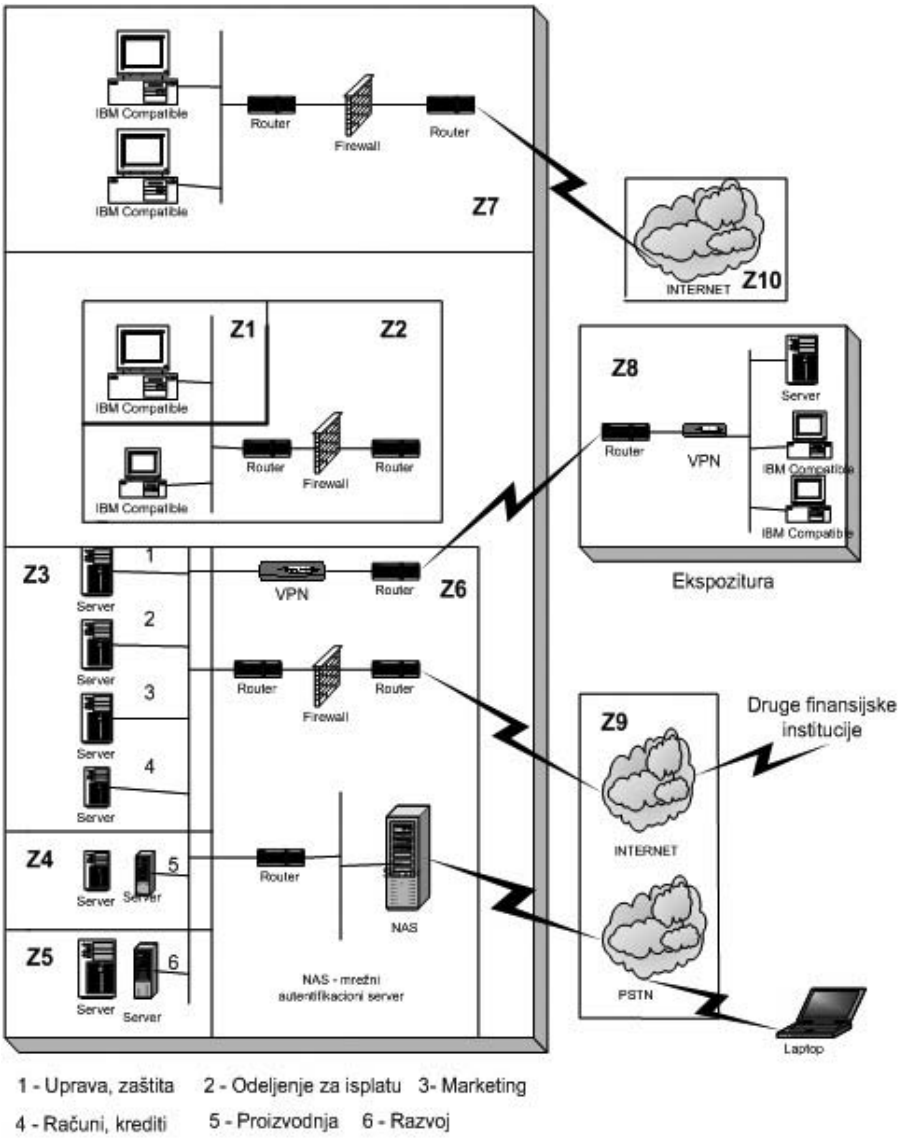
Standard	*Opis*
FIPS 199 (Feb 2004)	*Standards for Security Categorization of Federal Information and IS*
FIPS 200 (Mar 2006)	*Minimum Security Requirements for Federal Information and IS*
FIPS 201 (Feb 2005)	*Personal Identity Verification for Federal Employees and Contractors.*
ACSI33	*The Australian Government Information and Communications Technology Security Manual (unclassified version).*
SS507 Singapore Standards	*Covers "Business Continuity/Disaster Recovery (BC/DR) Service Providers". It is being used as the base/donor document for ISO 27006.*

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

PRILOG 3.

PRIMER BEZBEDNOSNE KATEGORIZACIJE OBJEKATA VELIKOG IKTS

1. korak*:* struktura banke deli se u deset *bezbednosnih zona* prema kriterijumu u opisu zone:



Sl. P3.1. Bezbednosne kategorije velike banke

Bezb. zona	Kriterijum klasifikacije
1 i 2.	Uprava i odeljenje *za* zaštitu imaju sopstvene interne servere. Koriste zajednički segment LAN, ali rade nezavisno i dele malo podataka. Zahtevaju uvid u podatke drugih odeljenja, kroz organizovani proces. Uprava podatke iz odeljenja za zaštitu dobija u vidu izveštaja. Zato se modeluju kao dve odvojene zone.
3.	Odeljenja se grupišu na bazi podataka koje procesiraju. Svi ovi departmani zahtevaju obiman pristup podacima klijenata iz različitih razloga.
4.	Proizvodni sistem sadrži sve zajedničke resurse, proizvodne aplikacije i podatke, uzima podatke sa servera smeštenih u departmanima kroz transfer podataka u realnom vremenu ili kroz ***batch***–orijentisan proces. Pošto sadrži glavne kopije svih proizvedenih podataka, zaštita ove zone je kritična za uspeh banke.
5.	Departman za razvoj LANa ne sadrži proizvodne podatke, ali za testiranja u IS može zahtevati neke proizvodne podatke, što komplikuje proces zaštite te zone.
6.	Obuhvata svu infrastrukturu za povezivanje, koja nije spojena na Internet.
7.	Uključuje sve uređaje za pristup Internetu. Distinkcija između ove dve zone napravljena je iz razloga nasleđa različitih IKTS.
8.	Izdvojena podružnica banke, ima lokalni server, koji čuva podatke lokalnih klijenata i radnih stanica, ažurira centralnu banku i prima ažurne podatke iz nje kroz noćnu razmenu formatiranih datoteka.
9.	Pokriva spoljnu mrežnu infrastrukturu, koju obezbeđuje TTPS provajder.
10.	Pokriva mrežnu infrastrukturu koja obezbeđuje vezu sa Internetom.

2. korak: identifikacija različitih tipova sistema u svakoj zoni i klasifikacija sistema na bazi bezbednosnih zahteva; klase se tabelarno prikažu, a zatim se ispitaju postojeći tokovi podataka između zona, koncentrišući se na najvažnije tokove; najvažniji tokovi se sumiraju i tabelarno prikažu; na prethodnom modelu vrši se analiza rizika.

3. korak*:* izbor i implementacija adekvatnih kontrola zaštite.

Prednosti strukturnog modela bezbednosnih zona: bezbednosne zone omogućavaju da se o specifičnim problemima diskutuje sa odgovarajućim osobljem; klasifikovanjem sistema u zone redukovan je broj sistema koje treba analizirati i broj radnih stanica i servera sa oko 2150 na svega 25 tipova sistema i stanica; ključni tokovi informacija između klasifikovanih grupa sistema korisni su za donošenje odluke za implementaciju kontrola zaštite i određivanje vrste poverljivih odnosa koje treba uspostaviti u organizaciji.

PRILOG 4.

METOD POKRIVANJA PRETNJI KONTROLAMA ZAŠTITE

Procena pokrivanja pretnji vrši se za ***tri osnovna efekta,*** indicirana sa jednim od simbola:

1. **„√" –** kontrola zaštite obezbeđuju adekvatnu zaštitu i pokrivanje datih pretnji**;**
2. **„√-„ –** kombinacija kontrola zaštite u datom sistemu osnovne zaštite i kontekstu u kojem se kontrole koriste, uključujući sve opšte faktore smanjenja rizika, obezbeđuje adekvatnu zaštitu i pokrivanje navedenih pretnji **i**
3. **„X" –** kontrola zaštite u izabranom osnovnom sistemu zaštite ne obezbeđuju adekvatno pokrivanje navedenih pretnji.

Tabela P4.1. Procena pokrivanja grešaka i prirodnih događaja osnovnim kontrolama zaštite

Karakteristike pretnje	**Procenjeno pokrivanje osnovnih kontrola zaštite**		
	NISKO	**SREDNJE**	**VISOKO**
Greške (mašinske ili ljudske)	√–	√–	TBD
Prirodni događaji			
Ometanje	√–	√	TBD
Lokalna nesreća	X	√	TBD
Regionalna katastrofa	X	X	TBD

Legenda		
	√	Kontrole zaštite u izabranoj osnovnoj zaštiti koje obezbeđuju adekvatno bezbednosno pokrivanje za identifikovane pretnje
	√–	Kombinacija kontrola zaštite u izabranoj osnovnoj zaštiti i kontekstu u kojem se koriste, uključujući sve faktore smanjenja rizika, koje obezbeđuju adekvatno pokrivanje za identifikovane pretnje
	X	Kontrole zaštite u izabranoj osnovnoj zaštiti, koje ne obezbeđuju adekvatno bezbednosno pokrivanje za identifikovane pretnje
	TBD	Treba da bude definisan

Tabela P4.2. Procenjeno pokrivanje osnovne zaštite za lokalne napade

Karakteristike pretnje	Procenjeno pokrivanje osnovnih kontrola zaštite		
	NISKO	SREDNJE	VISOKO
Namerni napad: LOKALNI			
Sofistikacija napada: NISKA	√	√	TBD
Sofistikacija napada: VISOKA			
Namera napadača: NEMALICIOZNA			
Resursi napadača: SVI NIVOI (MINIMALNI; PROSEČNI; VISOKI)			
Pristup napadača: AUTSAJDER	√	√	TBD
Pristup napadača: INSAJDER	√–	√–	TBD
Namera napadača: MALICIOZNA			
Resursi napadača: MINIMALNI			
Pristup napadača: AUTSAJDER	√	√	TBD
Pristup napadača: INSAJDER	√–	√–	TBD
Resursi napadača: PROSEČNI			
Pristup napadača: AUTSAJDER	√	√	TBD
Pristup napadača: INSAJDER	√–	X	TBD
Resursi napadača: ZNAČAJNI			
Pristup napadača: AUTSAJDER	√	√	TBD
Pristup napadača: INSAJDER	√–	X	TBD

Tabela P4.3. Procenjeno pokrivanje osnovne zaštite za mrežne napade

Karakteristike pretnje	Procenjeno pokrivanje osnovnih kontrola zaštite		
	NISKO	SREDNJE	VISOKO
Namerni napad: MREŽNI			
Sofistikacija napada: NISKA	√	√	TBD
Sofistikacija napada: VISOKA			
Namera napadača: NEMALICIOZNA			
Resursi napadača: SVI NIVOI (MINIMALNI; PROSEČNI; VISOKI)			
Pristup napadača: AUTSAJDER	√–	√–	TBD
Pristup napadača: INSAJDER	√–	√–	TBD
Namera napadača: MALICIOZNA			
Resursi napadača: MINIMALNI			
Pristup napadača: AUTSAJDER	√–	X	TBD
Pristup napadača: INSAJDER	√–	X	TBD
Resursi napadača: PROSEČNI			
Pristup napadača: AUTSAJDER	√–	X	TBD
Pristup napadača: INSAJDER	X	X	TBD
Resursi napadača: ZNAČAJNI			
Pristup napadača: AUTSAJDER	X	X	TBD
Pristup napadača: INSAJDER	X	X	TBD

PRILOG 5.

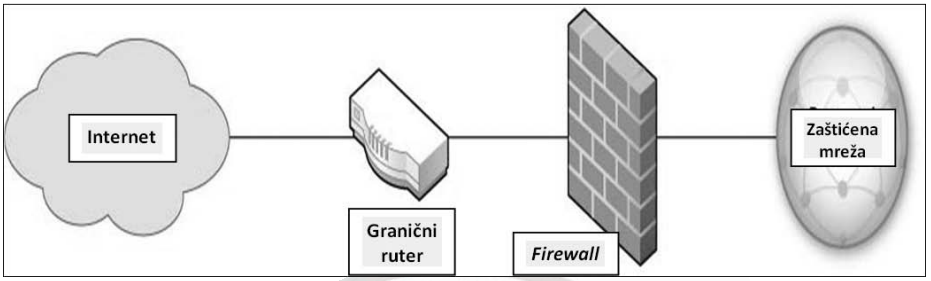
KRATKA ISTORIJA MALICIOZNIH PROGRAMA

Tabela P5.1. Kratka istorija malicioznih programa

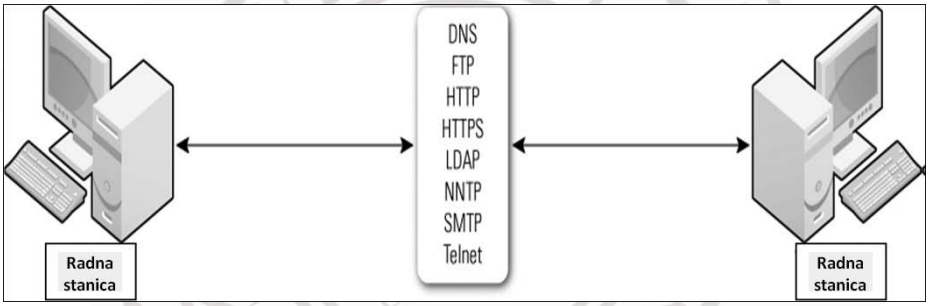
Godina	Podaci o kompjuterskim virusima
1962.	U Bel–u *Robert Moris*, stariji, razvio igru *Darwin*, koja se ponašala kao virus; zatim su se pojavili *PERVADE* [20], *Elk Cloner* [21], *Core War* [22] itd.
1981/2.	Prvi dokumentovani virusi, u igrama za *Apple II* otkrivena su najmanje tri virusa, uključujući i *Elk Cloner*–a; reč *virus* još se nije koristila za ovakav maliciozni kôd
1983.	Formalna definicija virusa, Fred Cohen: "Program koji može da zarazi druge programe tako što ih menja da sadrže izmenjenu verziju samog sebe." [9]
1986.	Prvi PC virus – *Brain,* inficirao *Microsoft DOS* sisteme; širio se preko *boot* sektora diskete i menjao ime diskete.
1988.	*Robert Moris* je oslobodio primitivnog crva i stopirao rad 10% Interneta.
1990.	Prvi polimorfni virusi koji izbegavaju AVP; menjaju se svaki put kod pokretanja.
1991.	*Virus Construction Set* (VCS), preko BBS–a i omogućio lako pravljenje virusa.
1992.	*Globe* virus, aktiviran u Windows OS; dodeljuje .exe ekstenziju .com datoteci.
1994.	*Good Times* lažni virus, izazvao veliku paniku; poznata štete od virusa.
1995/6.	Prvi makro virusi; pojava *netcat*–a za UNIX OS, danas se koristi kao *backdoor.*
1998.	*StrangeBrew*, prvi Java virus, inficirao druge Java programe, ugrozio Internet aplikacije.
1998.	Pojava *netcat*–a za Windows operativne sisteme.
1998.	*Back Orifice*, *backdoor* za udaljenu administraciju Windows OS.
1999.	*Melissa* makro virus/crv, napada Word dokumente; širi se putem e.maila; funkcioniše u MS Word 97, 2000 i MS Outlook 97 ili 98 e.mail klijentu
1999.	*Back Orifice 2000* (BO2K), GUI interfejs, API za kontrolu miša/tastature/ekrana.
1999.	*Knark Kernel–Level RootKit*, za skrivanja fajlova i procesa RM u kernelu Linux OS.
2000.	*Love Bug*, VBScript širi se preko ranjivosti Microsoft Outlook–a.
2001.	*Code Red* crv, koristi *buffer overflow* ranjivost IIS Web servera; preko 250.000 mašina su postale žrtve za manje od osam sati.
2001.	*Kernel Intrusion System*, revoluciju u *rutkit* manipulaciji kernelom Linux OS uvođenjem GUI–a i jako efektivnih mehanizama za sakrivanje.
2001.	*Nimda* crv koristi ranjivosti u MS proizvodima, kompromitovao preko 86.000 računara, naneo više od 635 miliona dolara štete; stvara *Guest* nalog sa administratorskim privilegijama i kompromituje računar.
2003.	*SQL Slammer* UDP crv; zarazio 75.000 računara za manje od 10 minuta.
2004.	*Santy* crv, koji je prvi koristio *Google* za pronalaženje novih žrtava.
2006.	16. februar, otkriven je prvi maliciozni softver za Mac OS X, trojanac *OSX/Lear.*
2007.	*Storm* crv, pravi bot mrežu; za šest meseci inficirao oko 1.7 miliona računara.
2008.	*Koobface* crv, širi se preko *Facebook* i *MySpace*–a.
2009.	*Conficker* crv zarazio preko 20 miliona MS servera; MS ponudio 250.000 US$ za hapšenje autora crva; do masovnog DoS napada nije došlo do 31. 05.2009.

PRILOG 6.

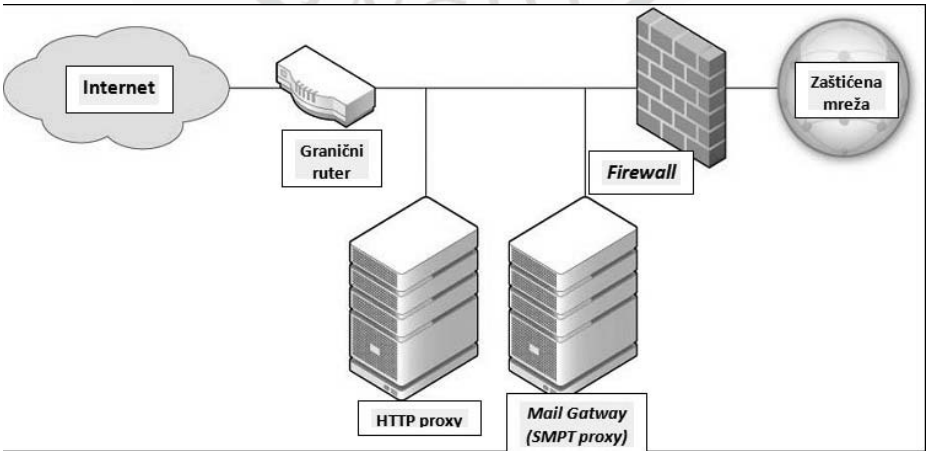
PRIMERI KONFIGURACIJE LOGIČKE BARIJERE U RAČUNARSKOJ MREŽI



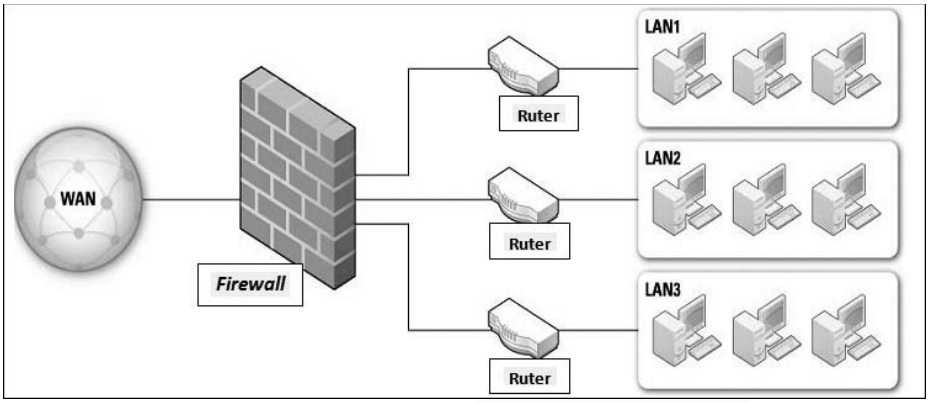
Sl. P6.1. Filter paketa korišćen kao granični ruter



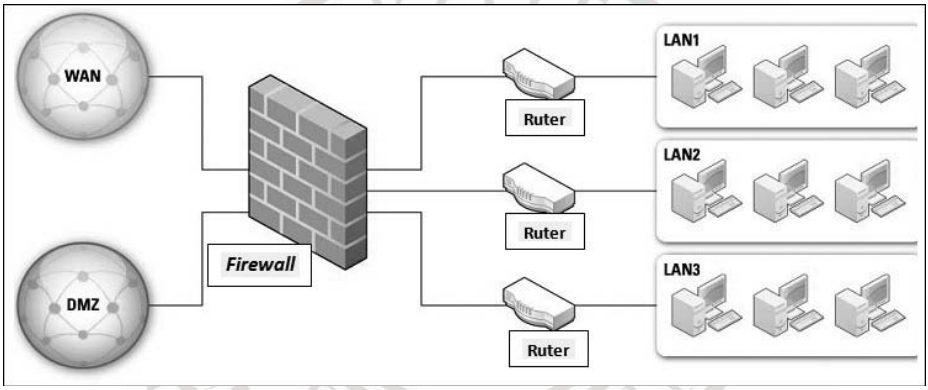
Sl. P6.2. Tipični proksi agenti



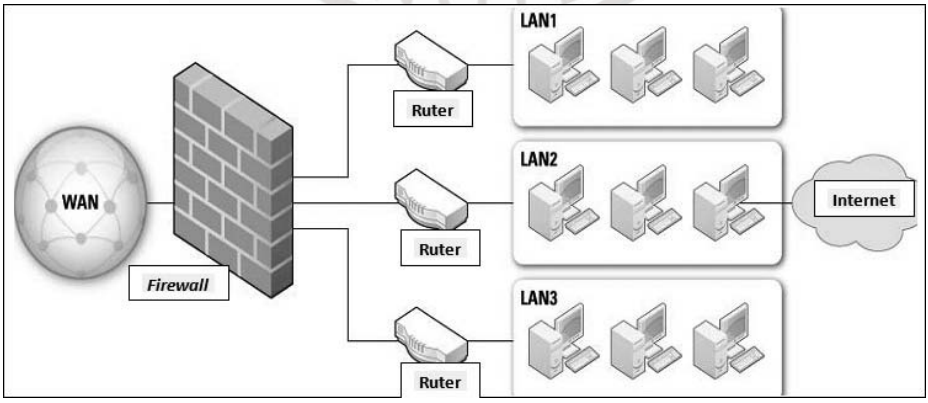
Sl. P6.3. Konfiguracija aplikativnog proksija



Sl. P6.4. Jednostavna rutirana mreža sa logičkom barijerom



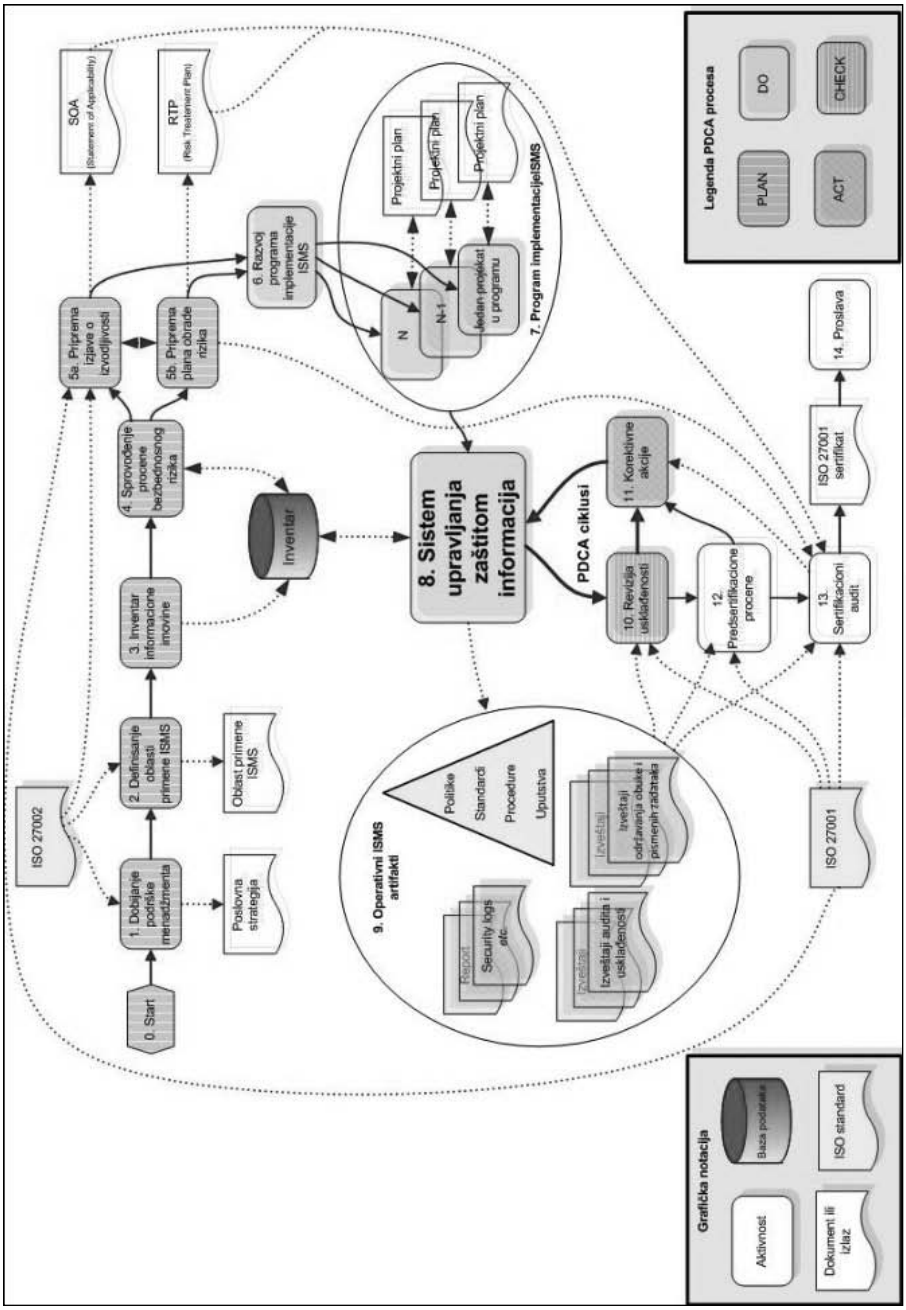
Sl. P6.5. Logička barijera sa DMZ



Sl. P6.6. Mreža sa drugom vezom spolja

PRILOG 7.

GRAFIČKI MODEL IMPLEMENTACIJE ISMS



Sl. P7.1. Grafički funkcionalni model implementacije ISMS

PRILOG 8.

TIPIČNI PAROVI RANJIVOST/PRETNJA (V/T)

Tabela P8.1. Tipični parovi ranjivost/pretnja

Ranjivost – V	Pretnja – T koja je može iskoristiti
Okruženja i infrastrukture	
Nedostatak fizičke zaštite zgrade, vrata i prozora	Krađa
Neadekvatne upotreba AC zgradama i sobama	Krađa, namerno oštećenje
Nestabilna električna mreža	Fluktuacija napona napajanja
Lokacija u oblasti podložnoj poplavi	Poplava
Hardver	
Nedostatak šeme periodične zamene (zanavljanja)	Kvar medija za skladištenje
Osetljivost na varijacije napona napajanja	Fluktuacija napona
Osetljivost na varijacije temperature	Eksterne temperature
Osetljivost na vlagu, prašinu, prljavštinu	Prašina
Osetljivost na EM zračenje	Izvori EM zračenja
Loše održavanje/pogrešna instalacija medija za skladištenje	Greška održavanja
Nedovoljno efikasna kontrola upravljanja konfiguracijom	Greška operatera
Softver	
Nedovoljan/nekompletan profil korisnika	Pad softvera
Bez ili nedovoljno testiranje softvera	Neovlašćena upotreba softvera
Komplikovan korisnički interfejs	Greška operatera
Nedostatak mehanizama I&A	Krađa identiteta legitimnih korisnika
Nedostatak kontrolnih tragova (*audit trail*)	Neovlašćena upotreba softvera
Poznata greška (bag) u softveru	Neovlašćena upotreba softvera
Nezaštićena lista pasvorda	Krađa identiteta korisnika
Loše upravljanje lozinkom	Krađa identiteta korisnika
Pogrešna alokacija prava pristupa	Neovlašćena upotreba softvera
Nekontrolisano preuzimanje i upotreba sw	Maliciozni kôdovi
Ulogovan posle napuštanja radne stanice	Neovlašćena upotreba softvera
Nedostatak efektivne kontrole promena	Pad softvera
Nedostatak dokumentacije	Greške operatera
Nedostatak rezervnih kopija (bekapa)	Maliciozni programi ili požar
Odlaganje/upotreba medija bez saniranja	Zloupotreba podataka i informacija
Omogućen nepotreban servis	Upotreba neovlašćenog softvera
Nezreo ili novi softver	Nekompetentno testiranje
Široko distribuirani softver	Gubitak integriteta u procesu distribucije

Ranjivost – V	Pretnja – T koja je može iskoristiti
Komunikacije	
Nezaštićene komunikacione linije	Prisluškivanje –oticanje informacija
Loše spajanje kablova	Infiltracija u komunikacione linije
Nedostatak I&A pošiljaoca i primaoca	Krađa identiteta korisnika
Otvoren prenos pasvorda	Mrežni pristup ilegalnog korisnika
Nedostatak dokaza o slanju i prijemu poruka	Poricanje transakcije
Dial–up linije	Mrežni pristup ilegalnog korisnika
Nezaštićen prenos osetljivih informacija	Prisluškivanje
Neadekvatno upravljanje mrežom	Preopterećenje saobraćaja
Nezaštićene konekcija javne mreže	Neovlašćeno korišćenje softvera
Nebezbedna mrežna arhitektura	Upad u mrežu
Dokumentacija	
Nezaštićeno skladište	Krađa
Nebriga kod odlaganja	Krađa
Nekontrolisano kopiranje	Krađa
Personal	
Odsustvo zaposlenih	Nedostatak radnika
Nekontrolisanje rada od strane obezbeđenja	Krađa
Nedovoljna bezbednosna obuka	Greška operativnog osoblja
Nedostatak svesti o potrebi zaštite	Greške korisnika
Nekorektno korišćenje softvera i hardvera	Greška operativnog osoblja
Nedostatak mehanizama za monitorisanje	Neovlašćeno korišćenje softvera
Nedostatak politike za zaštitu prenosa podataka	Neovlašćeno korišćenje RM
Neadekvatna procedura za prijem radnika	Namerna šteta
Proceduralne	
Nedostatak ovlašćenja za procesiranje informacija	Namerno oštećenje
Nedostatak procesa za ovlašćenje pristupa javnim inform.	Korupcija podataka
Nedostatak procesa za reviziju (superviziju) prava pristupa	Neovlašćeni pristup
Nedostatak procedure za kontrolu ISMS dokumentacije	Korupcija podataka
Nedostatak formalne procedure za registraciju korisnika	Neovlašćeni pristup
Nedostatak kontrole inventara imovine	Krađa
Nedostatak politike upotrebe mobilnog računara	Krađa
Nedostatak formalne procedure supervizije ISMS zapisa	Korupcija podataka
Nedostatak politike „čist sto i čist ekran“	Krađa informacija
Nedostatak/nedovoljna zaštita od kupaca i/ili TTP	Neovlašćeni pristup
Nedostatak/nedovoljna zaštita od zaposlenih	Krađa i prevara
Nedostatak planova za kontinuitet poslovanja	Tehnički kvarovi

Ranjivost – V	Pretnja – T koja je može iskoristiti
Nedostatak propisne alokacije odgovornosti u zaštiti	Poricanje transakcija
Nedostatak procedure za identifikaciju i procenu rizika	Neovlašćeni pristup IKTS
Nedostatak politike upotrebe e–pošte	Pogrešno rutiranje poruka
Nedostatak procedura za rukovanje klasifikovanih inform.	Greške korisnička
Nedostatak procedure za zaštitu intelektualne svojine	Krađa informacija
Nedostatak procedure za izveštaje o slabostima zaštite	Ilegalna upotreba RM
Nedostatak procedure za uvođenje softvera u OS	Greška operatera
Nedostatak procedure za kontrolu promena	Greška u održavanju
Nedostatak regularnog *auditing–a*	Neovlašćeni pristup
Nedostatak regularne revizije upravljanja	Zloupotreba resursa
Nedostatak mehanizama za nadzor proboja sistema	Namerna oštećenja
Nedostatak odgovornosti u zaštiti u opisu posla	Greška korisnika
Nedostatak evidencija grešaka u log datotekama	Neovlašćena upotreba soft-vera
Nedostatak evidencija grešaka u log datotekama	Greške operatera
Nedostatak definisanih procesa za upravljanje incidentom	Krađa informacija
Opšte ranjivosti poslovnih aplikacija za procesiranje	
Nekorektno podešavanje parametara	Korisnička greška
Primena aplikativnih programa na pogrešne podatke	Neraspoloživost podataka
Nemogućnost izrade izveštaja o upravljanju	Neovlašćeni pristup
Netačni podaci	Korisnička greška
Opšte primenljive ranjivosti	
Greška u jednoj tački	Pad komunikacionog servisa
Neadekvatan servis za održavanje	Kvar hardvera
Nepropisno projektovan i loš rad sa sistemom zaštite	Intercepcija i prisluškivanje veza

Primer estimacije ranjivosti informacione imovine

Prisustvo ranjivosti samo po sebi ne izaziva štetu sistemu. Ranjivost je stanje ili skup stanja, koji dopušta da je neki napad iskoristi i nanese štetu informacionoj imovini. Kao rezultat događaja jedne ili više pretnji (T), ranjivost (V) se rangira u odnosu na: intenzitet uticaja – **Ti** i potencijalnu izloženost gubicima – verovatnoću da će pretnje iskoristiti ranjivosti i uticati na imovinu – **Pu**, (NIST FIPS 800–30).

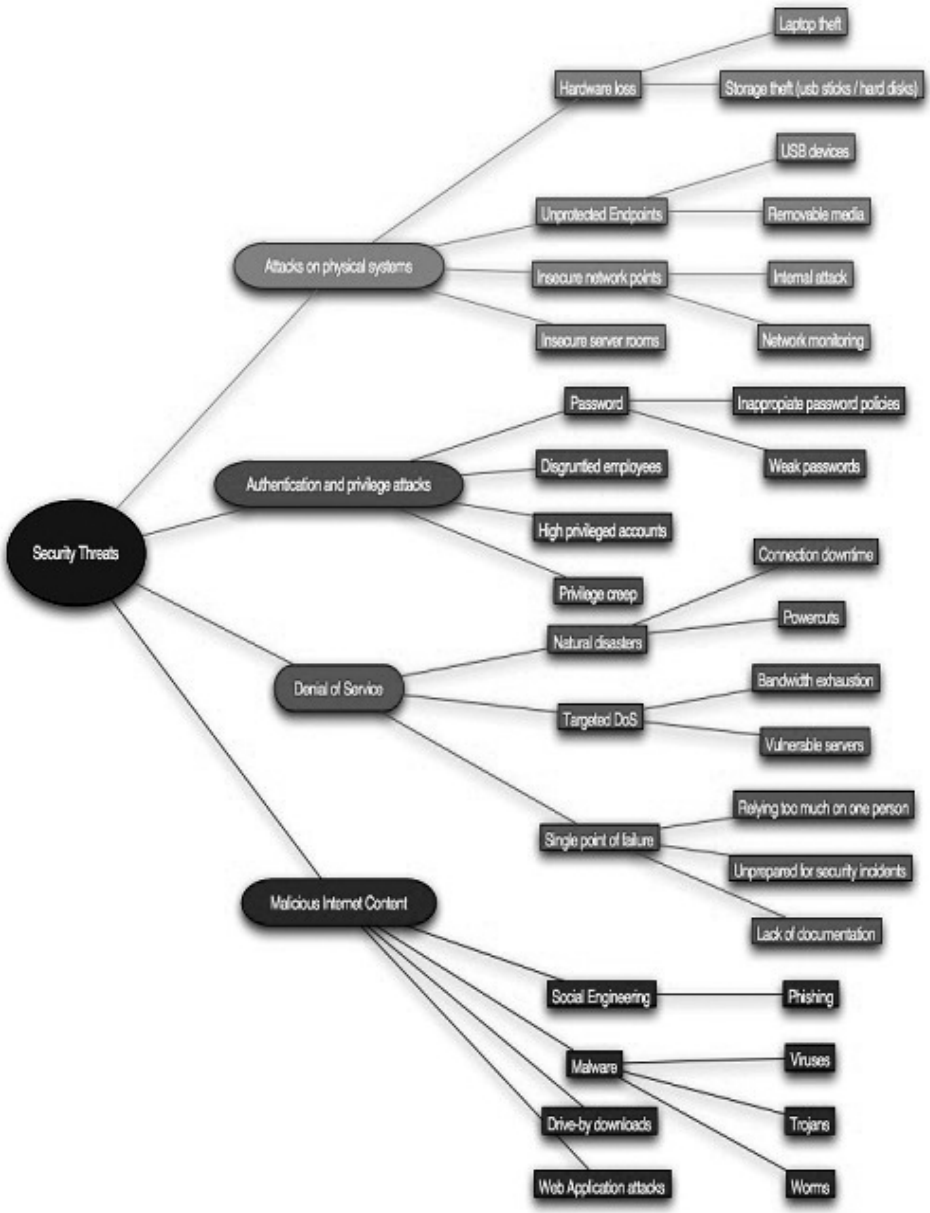
Tabela P8.2. Primer *skale rangiranja* ukupnih ranjivosti IKTS

Opis	***Skala***
Proboj može rezultirati u neznatnim gubicima i povredama sistema.	**1**
Proboj može rezultirati u malim gubicima ili povredama sistema.	**2**
Proboj može rezultirati u ozbiljnim gubicama i povredama sistema, a poslovi mogu biti ugroženi.	**3**
Proboj može rezultirati u vrlo ozbiljnim gubicima i povredama sistema, a poslovi mogu propasti.	**4**
Proboj može rezultirati u vrlo visokim novčanim gubicima, ili u izuzetno ozbiljne povrede pojedinaca ili organizacije (reputacije, privatnosti, konkurentske pozicije), a poslovi mogu propasti.	**5**

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

PRILOG 9.

TAKSONOMIJA BEZBEDNOSNIH PRETNJI – STABLO PRETNJI



I. TIPOVI UOBIČAJENIH PRETNJI (ISO/IEC 27005)

Sledeća lista, poređane u alfabetskom redosledu ne prema prioritetima, daje primer tipičnih relevantnih pretnji, gde *agenti* pretnje mogu biti: **D** – *namerna akcija prema informacionoj imovini*, **A** – *slučajna ljudska akcija, koja može oštetiti informacionu imovinu*, **E –** *prirodni događaj bez uticaja čoveka*

Tabela P9.1. Tipovi uobičajenih pretnji (ISO/IEC 27005)

Kvar erkondišna	*A, D, E*
Bombaški napad	*A, D*
Intercepcija komunikacija	*D*
Oštećenje linija	*A, D*
Kvar medija za skladištenje	*E*
Prašina	*E*
Zemljotres	*E*
Prisluškivanje	*D*
Elektromagnetsko zračenje	*A, D, E*
Elektrostatički naboj	*E*
Ekstremne temperature i vlažnost	*A, D, E*
Pad komunikacionih (mrežnih) servisa)	*A, D*
Gubitak napajanja	*A, D, E*
Nestanak vode	*A, D, E*
Požar	*A, D*
Poplava	*A, D, E*
Kvar hardvera	*A*
Oluja	*E*
Ilegalni uvoz/izvoz softvera	*A, D*
Ilegalno korišćenje softvera	*A, D*
Industrijska aktivnost	*A, D*
Munja	*E*
Greška u održavanju	*A, D*
Maliciozni softver	*A, D*
lažiranje korisničkog identiteta	*D*
Pogrešno rutiranje poruka	*A*
Zloupotreba resursa	*A, D*
Pristup mreži neovlašćenih korisnika	*D*
Greška operativnog osoblja	*A, D*
Nestabilnost napona napajanja	*A, E*
Poricanje izvršene akcije	*D*
Ponovljeno rutiranje poruka	*D*
Pad programa	*A, D*
Nedostatak stručnog osoblja	*A, D*
Tehnički kvar mrežne komponente	*A*
Krađa	*D*
Analiza mrežnog saobraćaja	*D*
Preopterećenje mrežnog saobraćaja	*A, D*
Greške u prenosu	*A*
Neovlašćeno korišćenje medija za skladištenje	*D*
Oružani napad	*A, D*
Neovlašćeno korišćenje mrežnih kapaciteta	*D*
Korišćenje softvera od neovlašćenog korisnika	*A, D*
Korišćenje softvera na neovlašćen način	*A, D*
Korisničke greške	*A, D*
Namerno oštećenje	*D*

Tabela P9.2. Humani izvori pretnji (**H**)

Izvor pretnje [H]	Motivacija	Akcija agenta pretnje
Haker, kraker	Izazov, ego, frustracija, pobuna	Hakovanje, društveni inženjering upad u sistem, proboj, neovlašćeni pristup sistemu
Kompjuterski kriminalac	Destrukcija i ilegalno otkrivanje informacija, krađa novca, ilegalna izmena podataka	Kompjuterski kriminal, prevara (intercepcija, krađa identiteta itd) *spoofing* (skeniranje i njuškanje po sistemu), upad u sistem
Terorista	Ucena, destrukcija eksploatacija, osveta	Bombaški napad, informaciono ratovanje, napad na sistem (DDoS) proboj u sistem, prisluškivanje sistema
Industrijska špijunaža	Konkurentska prednost, ekonomska špijunaža	Ekonomska eksploatacija, krađa informacija, upad u ličnu privatnost društveni inženjering, upad u sistem neovlašćeni pristup sistemu (krađa...)
Napad insajdera (slabo obučen, nezadovoljan, maliciozan, otpušten zaposleni)	Znatiželja, ego, obaveštajni rad, novčana korist, osveta, nenamerna greška ili omaška	Napad ne zaposlenog, ucena, pretraživanje vlasničkih informacija, zloupotreba računara, prevare i krađe, korupcija informacija, unos korumpiranih ili falsifikovanih podataka, maliciozni kod, prodaja personalnih informacija, sistemski bagovi, upad u sistem, sabotaža, neovlašćeni pristup
Dodatne reference za taksonomije pretnji (ISO/IEC TR 15446 i Sekcija 4, NIST SP800–30).		

II. PRIMERI TAKSONOMIJA ZA ESTIMACIJU PRETNJI

Tabela P9.3. Frekvencija pojave pretnje (T_f) (NIST SP 800–30)

Skala rangiranja	Opis
Vrlo visok (VV)	> 100 puta godišnje
Visok (V)	između 10 i 100 puta godišnje
Srednji (S)	između 1 i 10 puta godišnje
Nizak (N)	između 0,1 i 1 put godišnje
Vrlo nizak (VN)	< 0,1 put godišnje (manje od 1 put na svakih 10godina)

Tabela 6.3. Kapacitet izvora pretnje

Skala rangiranja	Opis
Vrlo visok (VV)	> 2% od svih izvora pretnji
Visok (V)	u glavnih 16% od svih izvora pretnji
Srednji (S)	prosečna veština i resursi (između donjih 16% i glavnih 16%)
Nizak (N)	u donjih 16% od svih izvora pretnji
Vrlo nizak (VN)	poslednji 2% od svih izvora pretnji

Rangiranje agenata pretnji (NIST FIPS SP 800–30)

Agenti pretnji su entiteti koji mogu namerno ili nenamerno iskoristiti ranjivosti sistema i naneti štetu informacionoj imovini. Agente pretnje rangiramo u odnosu na:

Motivaciju – mera koja kombinuje potencijalnu korist agenta pretnje i resurse koji su mu na raspolaganju za izvršenje (nije faktor za prirodne fenomene):

Tabela P9.4. Rangiranje pretnji u odnosu na motivaciju

Rangiranje sposobnosti	**Rangiranje motivacije**		
	1	2	3
1	1	2	3
2	2	3	4
3	3	4	5

Kapacitet – mera sposobnosti i zahtevanog napora agenta pretnje da uspešno napadne IKTS koristeći njihove ranjivosti, a obuhvata: *tehniku, znanje, resurse, priliku*.

Tabela P9.5. Rangiranje kapaciteta i motivacije napadača

Kapacitet	**Skala**	**Motivacija**
Malo ili bez sposobnosti za preduzimanje napada.	**1 (N)**	Mala ili bez motivacije.
Umerene sposobnosti. Ima znanje i veštinu da preduzme napad ili mu nedostaje neko znanje, ali ima dovoljno resursa da preduzme napad.	**2 (S)**	Umeren nivo motivacije. Mogao bi delovati ako se pokrene/ provocira.
Vrlo sposoban. Ima znanje, veštinu i resurse da preduzme napad.	**3 (V)**	Visoko motivisan. Gotovo određen da preduzme napad.

Tabela P9.6. Rangiranje ukupnih agenata pretnji

Rang	**Opis**
1	Malo ili bez sposobnosti ili motivacije
2	Malo ili bez sposobnosti, umeren nivo motivacije; malo ili bez sposobnosti, visoko motivisan; umereno sposoban, umeren nivo motivacije
3	Veoma sposoban, umereno motivisan; umereno sposoban,umereno motivisan
4	Vrlo sposoban, umereno motivisan; umereno sposoban, vrlo motivisan
5	Vrlo sposoban, vrlo motivisan

Tabela P9.7. Proračun frekvencije pojave bezbednosnog incidenta–pretnje (T_f)

Skala rangiranja	Opis
Vrlo visok (VV)	> 100 puta godišnje
Visok (V)	između 10 i 100 puta godišnje
Srednji (S)	između 1 i 10 puta godišnje
Nizak (N)	između 0,1 i 1 put godišnje
Vrlo nizak (VN)	< 0,1 put godišnje (manje od 1 put na svakih 10godina)

Tabela P9.8. Kapacitet izvora pretnje

Skala rangiranja	Opis
Vrlo visok (VV)	> 2% od svih izvora pretnji
Visok (V)	u glavnih 16% od svih izvora pretnji
Srednji (S)	prosečna veština i resursi (između donjih 16% i najviših 16%)
Nizak (N)	u donjih 16% od svih izvora pretnji
Vrlo nizak (VN)	najnižih 2% od svih izvora pretnji

Preporuka za estimaciju faktora rizika za proračun *verovatnoće bezbednosnog incidenta (P_t)* u sledećoj tabeli može se korigovati po zahtevu vlasnika sistema:

Tabela P9.9. Proračun verovatnoće pojave incidenta – napada (realizacije pretnje) (*Pt*)

Nivo	Estimacija	Definicija
Vrlo visok	1	Vrlo visoka verovatnoća napada sve dok se ne primeni zaštita.
Visok	2	Smatra se da postoji visoka verovatnoća napada ako zaštita nije primenjena.
Srednji	3	Smatra se da postoji razumna verovatnoća napada.
Nizak	4	Smatra se da je rizik od napada nizak.
Vrlo nizak	5	Smatra se da postoji vrlo niska verovatnoća napada.

PRILOG 10.

PRIMERI ODREĐIVANJA VEROVATNOĆE I NEODREĐENOSTI PRETNJI

Tabela P10.1. Verovatnoća realizacije pretnje (P)		
Klasa	**Vrsta**	**P** (0–1) ili (0–5)
Aero zagađenje	Prašina, padavine, gasovi, smog, dim	
Modifikacija inf. imovine	Aplikativnog softvera, datoteka podataka, hardvera, sistemskog softvera, zaštitnog softvera	
Komunikacijske greške	Prekid veze, greške u radu/šum	
Kompromitacija sistema	Pristup agenta pretnje i bivših zaposlenih, nepropisno izdavanje i označavanje informacija, gubljenje dokumenata i medija, KEMZ, otvorena vrata/kontejner	
Kompromitacija lozinke	Fizički ulazak u prostor IKT sistema, tehnički prodor (prisluškivanje), neovlašćeni upad (haker)	
Tehnička greška	Unesena, operativnog rada, programiranja, prenosa	
Vatra	Lokalni požar, katastrofa/viša sila, eksplozija, spolja	
Upad/oštećenje	Provala, nelojalno osoblje, sabotaža, terorizam,	
Prevara/pronevera	Lažni izveštaj, pronevera, lažno predstavljanje/ulaz	
Geološki potresi	Zemljotres, klizište zemlje, vulkanska erupcija	
Greške hw u okruženju	Hlađenje, grejanje, ventilacija	
Oštećenja vodom	Prskanje cevi, curenje česmi, kiša–(krov, prozor), poplava	
Zabrane	Okupacija, evakuacija, epidemija, pobuna, obustava rada..	
Interferencija	EM, EMINE (EM impuls nuklearne eksplozije), radio opseg	
Gubitak inf/pod	Spolja, iznutra, neregularno	
Prekid napajanja	Spolja, iznutra, neregularno	
Zloupotreba IKT	Spolja, iznutra, neregularno	
Povrede/smrt	Nevreme/poledica, oluja/orkanski vetar, ciklon/tornado	
Statičko pražnjenje	Nevreme/poledica, oluja/orkanski vetar, ciklon/tornado	
Oštećenja	Nevreme/poledica, oluja/orkanski vetar, ciklon/tornado	
Pad sistema	Hardvera, softvera	
Krađa	Hardvera, softvera	

Tabela P10.2. Stepen neodređenosti pretnje (N)	
Definicija	**Mera verovatnoće pojave (V) i intenziteta manifestacije pretnje (I)**
Niska N: *V/I*	Postoje pouzdani statistički podaci o pretnjama (vatra i sl.)
Niska N: *I* Visoka N: *V*	Nije poznato kada će se pretnja dogoditi, ali je sigurno da će biti visokog intenziteta (neprijateljski napad i sl.)
Niska N: *V* Visoka N: *I*	Može se tačno predvideti pojava T, ali može biti beznačajna i/ili vrlo ozbiljna (npr. operaterska greška)
Srednja N: *V/I*	Statistički podaci su dosta retki, ali su srazmerno tačni (npr. krađa)
Visoka N: *V/I*	Informacije su vrlo zanimljive za širok krug ljudi (npr. poverljivi podaci)

I. slučaj estimacije (E) verovatnoće pojave pretnje (V):

- najpoznatiji, baziran na V za statistički praćene prirodne i veštačke događaje,
- obuhvata poplavu, oluju, kišu, sneg, ekstremnu temperaturu, požar i lokalni kriminal.

Tabela P10.3. I. slučaj estimacije–(E) verovatnoće pojave pretnji
Ako je: A – gornja granica (1), B – donja granica (0), E – opsega verovatnoće (0,1) biće:
a. *aritimetička sredina A* i *B*, ako se ceni da su vrednosti simetrično distribuirane u opsegu: *E=(A+B)/2*;
b. *geometrijska sredina A i B*, za vrednosti od dva i više redova veličine: *E=(AxB)1/2*
c. *harmonijska sredina A i B*, ako se veruje da je verovatnoća bliže B: *E=2(1/A+1/B)*
d. *Hurvicova sredina*, ako se želi izraziti vlastita pesimistička procena o tome kakva će verovatna pretnja biti; uvodi se Hurvicov procenat – H (od 1 do 100), (na primer: ako mislite da je verovatnoća niska staviti H=10 ili 20, a visoka – H=80 ili 90): *E=(HxA+(100–H)xB)/100*
e. *PERT estimacija*, ako su granice A i B istog reda veličine i ako se može proceniti najverovatnija vrednost M, koja može biti u skladu sa nekom poznatom situacijom i izraziti uverenje – D u M na skali od 1 – 10: *E=(A+DxM+B)/(D+2)*
f. *logaritamska PERT estimacija* se koristi, ako su opsezi A i B ≥2 reda veličine

II. slučaj estimacije (E) verovatnoće pojave pretnje (V):

- koristi se tamo gde postoji nizak stepen neodređenosti pretnji po intenzitetu (**I**), (npr. neprijateljski napad, jak zemljotres, i sl.) i visok stepen neodređenosti V,
- za estimaciju V koristi se veći broj slučajeva,
- procenjuje se verovatno vreme – **t** između pojava pretnje, a **E** verovatnoće je recipročna vrednost tog **t,**
- model je pogodan za **E** događaje koji se javljaju sa stepenom progresije od 10x3, tj. jedan put svakih 3 000 godina, 300 godina, 30 godina, 3 godine, sedmično, dnevno, na 10 minuta u toku dana, itd.

Tabela P10.4. Primer II. slučaja estimacije (E) verovatnoće pojave pretnji (V)		
Vreme	**Verovatnoća**	**Komparativni događaj**
dnevno	300	instalacija inicijalnog programa
sedmično	30	potpuno bekapovanje
sezonski	3	*up–grade* OS
na 3 god.	0,33	zamena IKTS (PC)
30 god.	0,033	rat
300 god.	0,0033	pad imperije
3000 god	0,00033	religiozno čudo
30 000 g.	0,000033	ljudska rasa
300000 g	0,0000033	geološko vreme

III. slučaj estimacije (E) verovatnoće pojave pretnji (V):

- koristi se gde je N stepen neodređenosti **V**, a visok stepen neodređenosti **I** (npr. operativna greška),
- za estimaciju intenziteta pretnji koristi se numerički sistem,
- za meru se uzima procenjeno vreme u čovek/sek. koje će verovatno biti izgubljeno zbog pada sistema i oporavka, a računa se od trenutka uticaja pretnje,
- za faktor progresije se može uzeti, takođe, faktor 10x3.

Tabela P10.5. Primer III. slučaja estimacije (E) verovatnoće pojave pretnje (V)		
vreme	intenzitet	komparativni događaj
3 sec	3	korekcija štamparske greške
30 sec	30	korekcija rečenice
5 min	300	restauracija datoteke
50 min	3 000	restauracija sistema aplikacija
9 h	30 000	restauracija OS
4 dana	300 000	restauracija baze podataka iz *back–up* sistema
40 dana	3 000000	restauracija baze podataka iz čvrste kopije

IV. slučaj estimacije (E) verovatnoće pojave pretnje (V):

- koristi se gde postoji umeren stepen neodređenosti **V** i **I** i gde postoje neki razbacani i nesređeni statistički podaci (npr. krađa),
- konstruiše se pretpostavljena statistička distribucija **V** i **I** pretnji,

- na uzorcima distribucije izvršiti estimaciju srednje vrednosti i standardne devijacije,

1. način simulacije: procene se maksimalne i minimalne moguće vrednosti V i I (A,B), prevede distribucija simuliranih podataka u ova dva opsega i izvuku uzorci iz distribucija,

- estimacija V i I može uzeti u obzir statističke podatke o procenjivanim pretnjama,
- kao baza simulacije koristi se *β (Beta*) distribucija i može se napraviti da *strmina* (odstupanje od srednje vrednosti najfrekventnije pojave) i *tok* (stepen glatkoće) simuliranih statističkih distribucija odgovaraju impresiji korisnika,

2. način simulacije je upotreba *Fuzzy* skupova: konstruišu se distribucije V događaja iz kojih se pomoću β distribucije u opsegu (0,1) sa parametrima oblikovanja (a,b) uzimaju slučajni uzorci,

- za prevođenje β distribucije u distribuciju simuliranih V ili I, treba mapirati prirodna stanja na linearnu decimalnu skalu,
- opseg simuliranih varijabli treba da bude dva reda veličine ili manji,
- da bi se generisala i oblikovala β distribucija, generišu se dve γ (gama) distribucije slučajnih varijabli–X1 i X2,
- X1 – aditivna konvolucija "a" negativne eksponencijalne slučajne promenljive sa srednjom vrednosti jednakom 0,1,
- X2 – aditivna konvolucija "b" eksponencijalne promenljive, (konvolucija – u ovom slučaju sabiranje i delenje u određenom trenutku),
- beta distribuirana slučajna varijabla X=X1/(X1+X2) je koeficijent konvolucije X1 i aditivne konvolucije X1 i X2.

Tabela P10.6. IV. slučaj estimacije (E) verovatnoće pojave pretnji (V)

Beta distribucija je približno zvonastog oblika koji se precizno formira izborom „***a***" i „***b***" parametara: *a* – visok, *b* – nizak pomera srednju vrednost prema 1; b – visok, a – nizak pomera srednju vrednost prema 0; a i b – jednaki, pomeraju srednju vrednost prema 0.5; ***a*** i ***b*** – visoki proizvode vršnu distribuciju; ***a*** i ***b*** – niski proizvode ravnu (glatku) distribuciju.
Parametarski par [***a,b***] bira se tako da reflektuje procenu menadžera o prirodi pretnje. Skala: H – visok, M – srednji, L – nizak, ima tri kvaliteta: M (veličina): visoka/niska V ili I pomera srednju vrednost desno/levo; H (obezbeđuje E): pomera srednju vrednost neznatno desno ili levo; C (poverenje u E): može biti visoko ili nisko, (vršna ili ravna kriva).
Može se generisati svih sto mogućih kombinacija *a* i *b* pošto svaki parametar oblikovanja varira od 1 – 10. Crtanjem rezultirajuće distribucije i izborom 27 kombinacija a i b koje daju dijagrame najbolje kombinacije M, H i C, može se generisati oblik distribucije po želji.

V. slučaj estimacije (E) verovatnoće pojave pretnji (V):

- koristi se gde postoji visoka neodređenost V i I i gde su informacije veoma zanimljive širokom krugu ljudi (npr. otkrivanje osetljivih informacija),
- u ovom modelu analitičar treba da pogađa korišćenjem „skale rangiranja" ili sa „premošćavanjem i podešavanjem".

Tabela P10.7. V. slučaj estimacije (E) verovatnoće pojave pretnji (V)
Skala rangiranja. kada kvalitativna E, koju naprave konsultanti ili menadžment, uđe u procenu V ili I pretnje, oni koji daju informacije moraju izabrati za procenjenu vrednost najbliži mogući broj na skali od 1 do 5. Zatim se ova skala prevede u prirodniju logaritamsku od 0 – 1 vremena i veličine, da bi se došlo do iskoristivih parametara: 0=0; 1=0,1586; 2=0,5000; 3=0,7126; 4=0,8747; 5=1
Napomena: ovo nije stvarna logaritamska skala zbog uvođenja vrednosti „0" za 0 slučajeva, umesto vrednosti nešto malo iznad „0".
Prenošenje i podešavanje: analitičar upoređuje T prema događajima čije su verovatnoće i intenziteti dobro poznati (npr. fatalnost motornih vozila) i podešavaju određivanjem faktora koliko puta je više ili manje verovatna pojava razmatrane T.

Tabela P10.8. Procena štete (*cost-benefit* – ekonomsko tehnička analiza rizika)	
1.	Obezbeđuje komparaciju godišnjih troškova zaštite IS prema ceni očekivanih godišnjih gubitaka – (OGG) i svodi svaku analizu rizika na novčanu vrednost.
2.	Ne prihvata se sistem zaštite ako su troškovi zaštite veći od **OGG = T x A; T –** verovatnoća pojave pretnje/godini, a **A** – vrednost objekta na koji se pretnja odnosi.
3.	Treba voditi statistiku i uraditi kompjutersku evaluaciju na realnim pokazateljima.
4.	Obavezno analizirati prednost protivnika, dobijenu nanošenjem nastale štete.
5.	Proceniti troškove projektovanja i nadgradnje oštećenog procesa/proizvoda IKTS.
6.	Proceniti cenu rada na uklanjanju negativnih posledica napada.

Za automatsku obradu, OO baza podataka stabla pretnji pohranjuju se u bazu podataka zajedno sa ocenom mere intenziteta **I** svakog faktora rizika sa finijom gradacijom.

Tabela P10.9. Finija gradacija verovatnoće pojave pretnji	
Zanemarljiva	Nije verovatno da će se dogoditi.
Vrlo niska	Verovatno će se dogoditi 2 – 3 puta svake pete godine.
Niska	Verovatno će se dogoditi jedan put svake godine ili manje.
Srednja	Verovatno će se dogoditi svakih šest meseci ili manje.
Visoka	Verovatno će se dogoditi jedan put svakog meseca ili manje.
Vrlo visoka	Verovatno će se dogoditi više puta svakog meseca ili manje.
Ekstremna	Verovatno će se dogoditi više puta svakog dana.

PRILOG 11.

METODI PROCENE UKUPNOG RIZIKA

Metod matrice rizika sa predefinisanim vrednostima (ISO/IEC 13335–3)

Vrednost fizičke imovine – A se procenjuje u odnosu na troškove zamene ili rekonstrukcije resursa (kvantitativna mera). Vrednost **programske *A*** se procenjuje isto kao fizička **A**. Vrednost **čiste** A se određuje intervjuisanjem vlasnika informacija (**IoS –** izjava o osetljivosti), koja pokriva l*ičnu bezbednost i podatke, normativne, pravosudne i dr. obaveze, komercijalni i ekonomski interes, finansijske i nematerijalne gubitke poslovnu politiku i operacije.* Sve kvantitativne vrednosti A se konvertuju u kvalitativne (**N, S, V)**. Primenjuju se kriterijumi za određivanje vrednosti informacija. Za procenu rizika koriste se tri parametra vrednosti: A, T i V. Svaka vrednost parametra se procenjuje u odnosu na moguće posledice (gubitke, štetu) – **uticaj**. Uticaj **T** se posmatra u odnosu na mogućnost iskorišćenja neke ranjivosti **V.** Svi parametri se kvantifikuju proizvoljnom gradacijom (**PREPORUKA: N=1, S=2, V=3**). **Taksonomija pretnji**: namerni napad, uticaj okruženja, greške ljudi i kvar opreme. **Kompletiranje parova pretnje -– ranjivosti (T/V)** za svaku grupu imovine **(A)** koji se upoređuju sa opsezima predefinisanih vrednosti.

Za kompletiranje matrice podaci se skupljaju intervjuom tehničkog osoblja, fizičkom kontrolom lokacije i revizijom dokumenata. Za svaku **A**, razmatra se **V** i korespondirajuća kombinovana **T.** Ako ima **V** bez korespondirajuće **T** nema tekućeg rizika **(mora se pratiti).** Odgovarajući **red** u matrici identifikuje se sa vrednosti **A.** Odgovarajuća **kolona** se identifikuje sa vrednosti **uticaja U –** posledicom **T/V** para. Veličina matrice rizika u pogledu broja **kategorija** (nivoa rangiranja) intenziteta **T, V** i **A** mogu se menjati po volji organizacije. **Primer** u dodatku standarda **ISO/IEC 13335-3):**

A: **0** (niska), **1** (značajna), **2** (srednja),**3** (visoka), **4** (vrlo visoka),

V: **0** (niska), **1** (srednja), **2** (visoka)

T: **0** (niska), **1** (srednja), **2** (visoka

R = A +V +T; Rmin=0; Rmax=8

(R – sve celobrojne vrednosti Rmin≤ Rmax, uključujući i njih.

Matrica predefinisanih vrednosti za procenu identifikuje za svaku kombinaciju relevantne mere nivoa **rizika** na skali od **1 – 8.** Vrednost faktora rizika stavlja se u matricu rizika na struktuiran način, (Tabela 1.1): Neka je: A=3, T=V, a V=N, faktor rizika R= $R = A +(T/ V)$= 5. Neka je: A=2, T=N, a V=H, faktor rizika R= $R = A +(T/ V)$= 4

Tabela P11.1 Matrica predefinisanih vrednosti za procenu rizika

	T	*0*			*1*			*2*		
A	**V**	***0***	***1***	*2*	**V**	***0***	***1***	*2*	**V**	***0***
	0	0	1	2	***0***	0	1	2	***0***	0
	1	1	2	3	***1***	1	2	3	***1***	1
	2	2	3	***4***	*2*	2	3	***4***	*2*	2
	3	3	4	5	***3***	3	4	5	***3***	3
	4	4	5	6	***4***	4	5	6	***4***	4

Metod rangiranja pretnji prema proceni rizika – merenjem rizika

Formalno se koriste samo dva parametra: **A** – uticaj na informacionu imovinu (= vrednosti A) i **Pu** – verovatnoća uticaja ostvarenja pretnje (iskorišćenja ranjivosti). Implicitno se podrazumeva da je *uticaj na informacionu imovinu (A) ekvivalentan njenoj vrednosti*. Prijetnje – T se procenjuju u odnosu na odgovarajuće ranjivosti–V (izloženost) i meri verovatnoćom uticaja (na A) – **Pu**. Moguće vrijednosti su u rasponu: 1 (mala) – 5 (vrlo velika). Nivo rizika određuje proizvod tih dvaju parametra: **R= AxPu**

Tabela P11.2. Matrica za rangiranje pretnji (kolona a) prema proceni rizika

Opis T (a)	**Uticaj (A) (b)**	**Verovatnoća (Pu) (c)**	**Nivo rizika (R) (d)**	**Rang pretnje (e)**
Pretnja A	5	2	10	2
Pretnja B	2	4	8	3
Pretnja C	3	5	15	1
Pretnja D	1	3	3	5
Pretnja E	4	1	4	4
Pretnja F	2	4	8	3

Tok procesa:

- Evaluirati vrednosti **A** prema predefinisanoj skali: **1 – 5** za svaku izloženost imovine **A** (kolona **b** u Tabeli), gde je **1** – najniža veličina
- Evaluirati verovatnoću događaja pretnje **Pu** prema predefinisanoj skali: **1 – 5** za svaku **T (**kolona **c** u Tabeli), gde je **1** – najniža veličina
- Proračunati nivo rizika **R=bxc (**kolona **d** u tabeli**)**
- Rangirati pretnje (faktore rizika) prema visini nivoa faktora rizika (kolona **e** u Tabeli)

Minimalna i maksimalna vrijednost procenjenog rizika iznose:

$$Rmin = Amin \times Pumin = 1,$$

$$Rmax = Amax \times Pumax = 25 .$$

Procenjeni rizik može poprimiti celobrojne vrednosti između Rmin i Rmax, uključujući i njih, ali isključujući proste brojeve izvan raspona vrijednosti i njihove višekratnike.

PREDNOSTI: metod omogućava: poređenje različitih **T** sa različitim uticajima na **A** i verovatnoćama događanja, rangiranje prema prioritetima ublažavanja, mogu se pridružiti i finansijske (kvantitativne) vrednosti ako je potrebno.

Tabela P11.3. Matrica nivoa rizika u ovom metodu sa preporučenom skalom rangiranja

Verovatnoća uticaja pretnje (Pu)	**Uticaj**		
	Nizak (N) (10)	**Srednji (S) (50)**	**Visok (V)(100)**
V (1,0)	N(10x1,0=10)	S(50x1,0=50)	V(100x1,0=100)
S (0,5)	N(10x0,5=5)	S(50x0,5=25)	V(100x0,5=50)
N (0.1)	N(10x0,1=1)	S(50x0,1=5)	V(100x0,1=10)

Rangiranje rizika: V (>50–100); S (>10–50); N (1–10)

Metod procene verovatnoće ostvarenja i mogućih posledica

Ovaj metod određuje posledice incidenata i prioritet pojedinih resursa.

Tok procesa metoda se sastoji od tri koraka:

- Dodeljuje se vrednost (**A**) svakoj informacionoj imovini, na bazi potencijalnog uticaja u slučaju realizacije neke prijetnje – incidenta (**Tp**). Za svaku A na koju je primenljiva neka T, pripisuje se vrednost A.
- Procenjuje se verovatnoća ostvarenja pretnje za neku ranjivost – uticaj (**U**). Ta verovatnoća predstavlja kombinaciju (**zbir**/proizvod) mogućnosti pojave pretnje (**Tp**) i lakoće iskorištavanja ranjivosti (**V**):

$$U = f(V,T)=V + Tp \text{ ili } U= VxTp$$

Tabela P11.4. Procene verovatnoće uticaja (ostvarenja pretnje) – **U**

Tp **(pretnja)**	0			1			**2**		
V **(ranjiv)**	0	**1**	2	0	**1**	2	0	**1**	2
U **(incid.)**	0	1	2	0	1	2	0	1	2

Težište je na uticaju incidenta – **U** i donošenju odluke kojom sistemu treba dati prioritet zaštite. Procenjuju se dve vrednosti za svaku **A** i **R** (rizik), čija kombinacija daje vrednost za svaku A.

Rizik se procjenjuje kao kombinacija vrednosti **A** i verovatnoće (pretnje) uticaja **U**:

$$R = f(A, U) = A + (V + Tp) = A + U$$

Rangiranje vrednosti za estimaciju rizika (**ISO/IEC 13335–3**):

A: 0 (niska), 1 (značajna), 2 (srednja), 3 (visoka), 4 (vrlo velika)

Tp: 0 (niska), 1 (srednja), 2 (visoka)

V: 0 (niska), 1 (srednja), 2 (visoka)

Tabela P11.5. Matrica za procenu rizika

U \ A	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	**1**	2	3	**4**	5
2	2	3	4	5	6
3	3	4	5	**6**	7
4	4	5	6	7	8

Vrednost u ćelijama matrice **(A/U)** se može koristiti za diferenciranje između delova imovine **A** koji čine sistem. Kada se sumiraju svi rezultati za pojedinačnu imovinu sistema, dobije se **A** sistema. Ovo se može iskoristiti za diferenciranje između sistema i donošenje odluke kojem sistemu dati prioritet zaštite. **Primer**: (sve vrednosti su slučajne, koriste se Tabele 1.1 i 1.2): neka sistem **S** ima: tri imovine **A1, A2 i A3** i dve pretnje **T1 i T2** primenljive na sistem S; neka je **A1=3, A2=2, A3=4;** neka je verovatnoća uticaja za A1, **T1 = N (0)**, a verovatnoća iskorišćenja ranjivosti (V)=S (**1**), tada je vrednost verovatnoće uticaja – U=**1** (Tabela 1.1). Rezultat kombinacije A1/T1 može se derivirati iz Tabele 1.2, kao presek vrednosti imovine A1=3 i vrednosti verovatnoće uticaja U=**1**, tj. vrednost nivoa rizika = **4.** Za A1/T2 neka je verovatnoća pretnje T2= S (**1**), a mogućnost iskorišćenja ranjivosti (V) = V (**2**) , biće (Tabela 1.1) U=**3**, iz Tabele 7.2 vrednost nivoa rizika je **6**. Sada se može računati totalni skor imovine **A1/T, tj. T=T1+T2,** koji iznosi **10**. Ovaj totalni skor imovine računa se za svaku posebnu imovinu i primenljivu pretnju. Totalni skor sistema (ST) računa se sumiranjem **A1T+A2T+A3T=ST**. Sada se različiti sistemi mogu uporediti i uspostaviti prioritet zaštite, kao i zaštite različite A u jednom sistemu. Ova analiza je primenjena za IKT sistem, ali može i za poslovne procese.

Metod distinkcije između prihvatljivog i neprihvatljivog rizika (HESTIA)

Određuje se u kojem je slučaju hitno potrebno reagovati na rizik, a kada se tretiranje rizika ne mora obaviti odmah. Prema ovoj metodi rizik može biti:

- **prihvatljiv (P)** ili
- **neprihvatljiv (N).**

Metoda odvajanja prihvatljivih i neprihvatljivih rizika predstavlja u stvari varijaciju metode tri – procena verovatnosti pretnji – mogućih posljedica (uticaja) ili metode 1 (matrica predefinisanih vrednosti). U ovom pristupu faktor rizika – **Ri** je:

Ri=A x Pu (vrednost imovine x verovatnoća uticaja)

Matrica prihvatljivih i neprihvatljivih rizika za estimaciju faktora rizika prema matrici 5x5 (1 do 5) sa rangiranjem A i Pu: *1 - nizak, 2 - značajan, 3 - srednji, 4 - srednje visok i 5 - visok*, prikazana je u Tabeli P11.6.

Tabela P11.6 Matrica prihvatljivih i neprihvatljivih rizika

Pu \ A	**1**	**2**	**3**	**4**	**5**
1	1	2	3	4	5
2	**2**	4	6	**8**	10
3	3	6	9	12	15
4	4	8	12	**16**	20
5	5	10	15	20	25

Procena rizika koristi se samo za rangiranje faktora rizika prema nivou štetnog uticaja, tako da se može odlučiti za koje se faktore rizika moraju primeniti hitne akcije, koji se mogu ublažiti sa manje rada i troškova, a koji se moraju samo pratiti (monitorisati). Liniju između prihvatljivog i neprihvatljivog rizika povlači vlasnik/menadžer sistema. U navedenom primeru prihvatljivi rizici (grupe rizika) su do nivoa 4; moraju se monitorisati i sukscesivno tretirati, svi rizici u opsegu 4 – 15; rizici u opsegu 15 – 16 su značajni i treba ih planski tretirati, a rizici u opsegu 20 – 25 su kritični i treba ih hitno tretirati.

PRILOG 12.

KONTROLNA LISTA PROCESA IMPLEMENTACIJE POLITIKE I PROCEDURA ZAŠTITE

Tabela P12.1. Kontrolna (ček) lista procesa implementacije politike i procedura zaštite

Kontrolna lista pitanja	DA	NE
Da li je od celokupne upravne strukture dobijena potpuna podrška za razvoj politike, standarda, uputstava i procedura zaštite?		
Da li je upravna struktura pokazala da je zaista ozbiljna u pogledu značaja podataka i informacija kao dragocenih objekata imovine organizacije i da potpuno veruje u program zaštite, kojeg je autorizovala, na odgovarajući način prezentirala svim zaposlenim i odobrila (naredila) implementaciju?		
Da li je obezbeđeno da sve kompetentne org. jedinice organizacije učestvuju u razvoju i realizaciji politike zaštite, svesno i sa osećanjem vlastite odgovornosti, da bi se reducirale prepreke i nerazumevanja? (IS, nadzor i kontrola, upravljanje rizikom, pravna i kadrovska pitanja, ključne korisničke organizacije su grupe koje treba uključiti).		
Da li su razmatrani faktori realne kulture i etičkih principa organizacije kao i drugi jedinstveni zahtevi u razvoju politike, standarda, uputstava i procedura zaštite?		
Da li su obezbeđeni uslovi za propisnu implementaciju rezultata procesa analize rizika paralelno sa razvojem politike, standarda, uputstava i procedura zaštite?		
Da li je upravna struktura preduzela korake da svi zaposleni budu svesni aktuelne promocije i implementacije politike, standarda, uputstava i procedura zaštite?		
Da li je u svakoj org. jedinica postavljen (imenovan, zadužen) predstavnik ili koordinator zaštite podataka i informacija?		
Da li je planirana obuka za sve kategorije zaposlenih radi podizanje svesti o potrebi i upoznavanja sa elementima politike, standarda, uputstava i procedura zaštite, posebno sa specifičnim dužnostima i odgovornostima u oblasti zaštite?		
Postoji li kontinualno ažuriranje politike, standarda, uputstava i procedura zaštite, da bi se obezbedila implementacija novih revidiranih zahteva organizacije?		
Da li se u cilju održavanja i ažuriranja svesti o potrebi zaštite redovno održavaju odgovarajući sastanci, publikuju brošure, posteri, objavljuju radovi u internim časopisima?		
Da li su specifičan pojedinac ili grupa zaduženi za implementaciju Programa zaštite organizacije?		

Odlukom Senata Univerziteta "Singidunum", Beograd, broj 636/08 od 12.06.2008, ovaj udžbenik je odobren kao osnovno nastavno sredstvo na studijskim programima koji se realizuju na integrisanim studijama Univerziteta "Singidunum".

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

007:004.056(075.8)

МИЛОСАВЉЕВИЋ, Милан, 1952-
Osnove zaštite informacija : metodološko-tehnološke osnove / Milan Milosavljević, Gojko Grubor. - Beograd : #Univerzitet #Singidunum, 2010 (Loznica : Mladost grup). - XIX, 370 str. : ilustr. ; 24 cm

Tiraž 300. - Bibliografija: str. 330-333.

ISBN 978-86-7912-313-8
1. Грубор, Гојко, 1949- [аутор]
а) Информациона технологија - Безбедност

COBISS.SR-ID 180526604

© 2010.

Sva prava zadržana. Ni jedan deo ove publikacije ne može biti reprodukovan u bilo kom vidu i putem bilo kog medija, u delovima ili celini bez prethodne pismene saglasnosti izdavača.